



16th Global Symposium for Regulators (Sharm el-Sheikh, 2016)

Be Empowered, Be Included!

Building Blocks for Smart Societies in a Connected World

Discussion Papers

This PDF is provided by the International Telecommunication Union (ITU) Library & Archives Service from an officially produced electronic file.

Ce PDF a été élaboré par le Service de la bibliothèque et des archives de l'Union internationale des télécommunications (UIT) à partir d'une publication officielle sous forme électronique.

Este documento PDF lo facilita el Servicio de Biblioteca y Archivos de la Unión Internacional de Telecomunicaciones (UIT) a partir de un archivo electrónico producido oficialmente.

یجرى نورکتلا فملنم تذخوماً ی هو ت اظوفحموال ٲمکتبال قسم ، (ITU) للاتصالات الدولي الاتحاد من مقدمة PDF ینسق النسخة هذه امیرسٲ إعداده.

本PDF版本由国际电信联盟（ITU）图书馆和档案服务室提供。来源为正式出版的电子文件。

Настоящий файл в формате PDF предоставлен библиотечно-архивной службой Международного союза электросвязи (МСЭ) на основе официально созданного электронного файла.

GSR-16 Discussion paper

Building Blocks for Smart Societies in a Connected World: A Regulatory Perspective on Fifth Generation Collaborative Regulation

Sofie Maddens, Head, Regulatory and Market Environment Division, BDT, ITU

May, 2016

Work in progress, for discussion purposes
Comments are welcome!

Please send your comments on this paper at: gsr@itu.int by 30 May 2016



This report was prepared by Ms Sofie Maddens, Head, ITU BDT Regulatory and Market Environment Division with input from Ms Youlia Lozanova.

Contents

1	Introduction.....	4
2	ICTs as Enablers of Smart Connected Societies.....	5
2.1	ICTs as an Enabler for the Achievement of the Sustainable Development Goals.....	6
2.2	ICTS as Enablers across the Sectors.....	7
2.2.1	Administration and ICTs	8
2.2.2	Agriculture and ICTs.....	10
2.2.3	Education and ICTS	10
2.2.4	Health and ICTS.....	11
2.2.5	Energy and ICTs	11
2.2.6	Digital Financial Services.....	12
3	Overview of ICT and Collaborative Regulatory Frameworks.....	14
3.1	Telecommunication/ICT Regulation	14
3.1.1	Evolution of ICT/Telecommunication Regulation.....	14
3.1.2	Mandate of ICT/Telecommunication Regulators	17
3.2	Interaction with Other Authorities.....	18
3.2.1	Broadcasting and Media Authorities.....	19
3.2.2	Competition authorities	20
3.2.3	Consumer Protection Agencies	21
3.2.4	Data Protection Agencies	22
5	Recommendations for Collaboration in a Smart Connected Society	26

1 Introduction

In today's converged digital environment, where ICTs and digital technologies are recognized as the foundation for economic and social development and the growth of smart connected societies, defining broad and innovative collaboration at the policy and regulatory level is a must. Recognition has grown that we need ecosystems that include ICT operators and service providers, but also various stakeholders from the health, education, financial services and other sectors as partners to connect the world and create value for individuals, businesses and communities.

As most sectors of society and the economy are increasingly intertwined, cross-sectoral collaboration is more than ever required along with innovative regulatory approaches such as co-regulation and self-regulation, leading to new forms of collaborative regulation. Essentially, the success of smart connected digital societies and their economy will rest on trust as well as on regulation. The success or failure of collaborative businesses revolves around user trust, and appropriate regulation is a key element in those new models. A plethora of technological developments offer opportunities, but also challenges and regulators and policy makers must be ready to address the issues. Through collaboration, telecommunication/ICTs together with broader technology developments can improve governance outcomes.

Understanding the challenges and needs of all the different stakeholders involved in building smart societies, including the evolution of the policy, regulatory, economic and financial frameworks across the economy, will provide policy makers and regulators with the understanding needed to move forward and develop holistic cross-sectoral legal and policy measures for a connected world.

Common principles that underpin and constitute the foundation of smart societies include innovation, openness, transparency, empowerment, participation, inclusiveness, efficiency, co-creation and sharing, as well as collaboration.

Common issues and barriers faced by stakeholders across the sectors include interoperability, security, data integrity and portability, privacy, reliability, transparency, trust, unequal level playing field, unfair competition (Significant Market Power), Quality of Service, and pricing.

By developing a collaborative approach to regulation, the various sector regulators can contribute to reducing the regulatory conundrum, overlap and duplication across the economy, and provide for greater coherence, predictability and trust in the digital ecosystem.

This paper will:

- Define the role of the ICT sector in achieving smart societies, ICTs being the foundation for the transformation across society and the economy, i.e., in health, education, utilities (transport, railways, roads, electricity, water and sanitation), various industries/manufacturing, e-government services, e-commerce, entertainment, environmental issues, etc.;
- Provide a high-level overview of the different regulatory frameworks in place that stakeholders have to comply with and which provide the framework to protect consumer rights (telecom and broadcasting regulation, competition law, utilities regulation, consumer protection law, etc.) and identify commonalities, differences, areas of regulatory overlap, duplication and potential areas for collaborative regulation;
- Define recommendations for collaboration to enable the deployment of smart societies, in particular on (1) the roles and responsibilities of the different stakeholders and in particular regulatory authorities, and their respective mandate; and (2) the regulatory measures/framework needed to foster the deployment of smart sustainable societies.

2 ICTs as Enablers of Smart Connected Societies

Today, we live in a connected society – a society where mobile, broadband, and cloud computing are transforming the fabric of society and hold the promise of great opportunities for all people. Yet, while the Internet of Everything is a dominant topic of interest to policy makers and regulators, billions are still unconnected, and this affects their ability to participate in the digital economy – socially, financially, and economically.

Technology and Infrastructure development is affecting our lives like never before. Digital services and tools have become an important part of who we are, and the future we once only saw in science fiction movies has already arrived. A truly networked society will lead to even more changes, with new behaviours, opportunities, and challenges. Added to that, it is also clear that the achievement of the 17 Sustainable Development Goals¹ will rely heavily on the digital ecosystem since there is an ever-expanding variety of services and applications to serve our social, business and entertainment needs.

The evolution in the sector has brought about changes – there are new players on the market and discussions as to new and existing business models, new technologies, and new opportunities. Regulators around the world have become more conscious of the changing ecosystem and are aware that they need to adapt to the changing environment. From a time when telecommunication/ICT regulators mainly focused on their creation as independent entities opening monopolistic markets, to one where they became active in promoting investment in infrastructure and services development and overseeing budding competitive markets, they now have many more issues at stake. Today, ICT regulators have become 4th Generation Regulators fostering the development of ICTs for economic and social development. We stand at the edge of 5th generation regulation where collaboration within the ICT sector and across the sectors is a reality.

In building smart connected societies and seeking to achieve the Sustainable Development Goals, policy makers, regulators and indeed all stakeholders are faced with similar concerns requiring common solutions. There is the recognition that there is the need to work together to create an enabling regulatory environment across the sectors and remove the barriers that hinder progress.

With the emergence of smart cities, smart nations, smart societies, ICT/telecommunication networks and services have become more efficient with the use of digital and telecommunication technologies, and this has benefitted people, businesses, and government. There are many opportunities, but this evolution is not without its challenges.

Collaboration within the sector and across sectors has led to the growth of the digital collaborative economy, allowing an even greater level of experimentation, innovation and growth than ever before. A strong digital economy is vital for innovation, growth, jobs and competitiveness. It offers opportunities but also challenges. The digital transformation is structurally changing the labour market and the nature of work. There are concerns that employment conditions, levels and income distribution will be affected by new digital applications and services, Artificial Intelligence, increased use of robots in manufacturing and service industries.

In the telecommunication sector, operators and service providers including carriers, OTTs and MVNOs are already starting to adopt a more collaborative approach, leveraging each other's expertise and resources to offer a wider range of services.

¹ Officially known as *Transforming our world: the 2030 Agenda for Sustainable Development*, the Sustainable Development Goals are contained in paragraph 54 United Nations Resolution A/RES/70/1 of 25 September 2015.

But the effect is wider. There is no doubt today that telecommunication/ICT is cross-cutting and an enabler for growth and development across the board.

The European Union Digital Single Market Strategy²

The European Union's 2015 Digital Single Market Strategy (DSMS) illustrates a cross-sectoral approach where ICTs are recognized as contributing to economic and social development, provided collaboration with other sectors and actors also takes place.

DSMS aims to offer opportunities for new start-ups and existing companies as well as for citizens by providing them with digital skills. DSMS also provides that enhanced use of digital technologies can improve citizens' access to information and culture, improve job opportunities and improve modern open government.

DSMS is built on three pillars:

Access: better access for consumers and businesses to digital goods and services across Europe;

Environment: creating the right conditions and a level playing field for digital networks and innovative services to flourish;

Economy & Society: maximizing the growth potential of the digital economy.

2.1 ICTs as an Enabler for the Achievement of the Sustainable Development Goals

The United Nations General Assembly in its resolution entitled "The Future We Want" provided that "The goal of sustainable development is to ensure the promotion of an economically, socially and environmentally sustainable future for the planet and for present and future generations. Sustainable development emphasizes a holistic, equitable and far-sighted approach in decision-making at all levels. It rests on integration and a balanced consideration of social, economic and environmental goals and objectives in both public and private decision-making. It emphasizes intra-generational and intergenerational equity".³ ICTs are at the core of such development.

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

A mapping exercise has been carried out that defines linkages of the World Summit on the Information Society (WSIS) Action Lines with the proposed SDGs to continue strengthening the impact of Information and Communication Technologies (ICTs) for sustainable development. Each UN Action Line Facilitator analyzed the connections and relations of their respective Action Line with the proposed SDGs and their targets. The goal of the mapping was to create a clear and direct link and an explicit connection between the key aim of the WSIS, that of harnessing the potential of ICTs to promote and realize the development goals, and the post 2015 development agenda, so as to contribute to the realization of the latter.⁴

² <http://ec.europa.eu/priorities/digital-single-market/>

³ (E/2013/69, para. 6)

⁴ <https://www.itu.int/net4/wsis/sdg/>

Some examples of how ICTs support the achievement of the SDGs include:

- **Goal No. 1** (No Poverty) for example, can be advanced through basic digital financial services which will lead to the inclusion of the poor in the digital economy. Ending poverty and ensuring that everyone has equal rights in economic resources, as well as access to basic services, is also key to the achievement of this Goal.
- **Goal No. 2** (Ending hunger) can be enhanced through ICTs by supporting countries to develop their e-agriculture strategies.
- **Goal No. 3** (Good Health and Well-Being) has seen great advancement through the evolution of mobile data applications. By mapping best practices on the role that eHealth applications can play in achieving the SDGs and developing national eHealth strategies, ICTs can be even better harnessed for health.
- **Goal No. 4** (Inclusive, equitable and lifelong learning opportunities for all) where integrated policies can play in fostering innovation in the education sector and facilitate the use of mobile technology for learning.
- **Goal No. 5** (Gender equality and empowering all women and girls) girls and young women can be encouraged to effectively use ICTs and consider careers in telecommunications/ICTs.
- **Goal No. 7** (Affordable, reliable, sustainable and modern energy for all) Making the grid more intelligent will require innovations that address legacy communications and the electrical infrastructure. Future grids will need to integrate sensors and smart meters in the distribution segment, distributed energy resources (DER) sites and homes to support demand/response, distributed generation and energy-aware applications. This implies big data as well as reliability and security of infrastructure.
- **Goal No.8** (Economic growth, productive employment, and decent work for all) can be enhanced by measures to empower users, for example through training on ICT-enabled entrepreneurship and promoting the use of new and existing telecommunication technologies for enhanced trade.
- **Goal No. 9** resilient infrastructure can be built, innovation achieved and inclusive and sustainable industrialization can be achieved through holistic and targeted ICT policies, regulations, and strategies as well as by promoting building confidence and security in the use of ICTs.

2.2 ICTS as Enablers across the Sectors

ICT sector players work more and more with non-traditional ICT players because ICTs are increasingly recognized an essential pillar of many areas of life in the converged ecosystem. School, government, health sector connectivity as well as digital financial inclusion require access to ICTs/telecommunications networks and services. The degree of telecommunications liberalization impacts other sectors, since market restrictions result in less competition, higher prices, poor quality of service and fewer connectivity options.

The benefits of market liberalization increase as more service providers enter the market and competition increases. However, not all the countries that have introduced a legal framework for a liberalized ICT market have succeeded in creating true competition. Continuing problems may stem from regulatory barriers to entry, including exclusivity clauses in the licenses held by existing operators, as well as ineffective or incomplete regulations on spectrum management, universal access, interconnection and even numbering.

Access to international infrastructure is also key to lowering the cost of bandwidth and broadband prices for consumers. It is important to establish effective interconnection and gateway regulatory frameworks that introduce new models of sharing and collocation and reduce barriers to existing private, government and international networks. Effective reforms can encourage existing providers and new market entrants to expand into broadband and other services and thus create the enabling environment by which ICTs/telecommunications can be a driver for economic and social development.

2.2.1 Administration and ICTs

E-Government

E-government is “the use of ICT and its application by the government for the provision of information and public services to the people” (Global E-Government Readiness Report 2004). More specifically, a 2014 UNDESA report refers to e-government as “the use and application of information technologies in public administration to streamline and integrate workflows and processes, to effectively manage data and information, enhance public service delivery, as well as expand communication channels for engagement and empowerment of people.”⁵

New technologies and applications such as cloud computing, mobile technologies as well as social media channels and apps have become part of the day-to-day life of people, business and society at local, regional and global level. More open governance through e-government has led to government becoming more transparent and accessible, which has led to more and new forms of public engagement and relationships.

Through the use of ICTs and digital platforms, e-Government increases public sector efficiency by facilitating interactions with public administrations, improving the quality of administrative services and processes and increasing transparency.⁶

Digital government or e-government strategies can bring governments closer to citizens and businesses. However, this requires access and connectivity, as well as digital skills, trust and confidence in the use of ICTs. Technology is not only a strategic driver for improving public sector efficiency, but can also create more open, transparent, innovative, participatory interactions with governments enhancing trustworthiness of governments within a digital connected society.

Ideally, a digital connected society where citizens have the skills to benefit from ICTs will lead to more collaborative and inclusive communications between government and regulators across the sectors, as well as between regulators and policy makers and other stakeholders such as citizens, business and non-governmental organizations.

Some examples include:

- On 18 April 2016 the European Commission published a Communication on Digitizing European Industry.⁷ Recognizing the role of technologies on public sector modernization and on the labour market, the Communication introduces policy measures, and calls for a human capital ready for the digital transformation with the necessary skills.

⁵ <https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/0ExecutiveSummary.pdf>

⁶ <https://ec.europa.eu/digital-single-market/en/news/communication-eu-egovernment-action-plan-2016-2020-accelerating-digital-transformation>

⁷ <https://ec.europa.eu/digital-single-market/en/news/communication-digitising-european-industry-reaping-full-benefits-digital-single-market>

-
- The Australian government recognizes that ICTs play a critical role in delivering and transforming the operations of government, and outlines the benefits that are expected to result from a strategic and coordinated approach to developing and use ICT in new, creative and innovative ways to deliver better, easier to use services in ways that best meet people's needs and expectations. The Australian Public Service (APS) ICT Strategy of 2012 provided that: "The APS will use ICT to increase public sector and national productivity by enabling the delivery of better government services for the Australian people, communities and business, improving the efficiency of APS operations and supporting open engagement to better inform decisions."⁸

Digitally enabled participation and the use of e-government services is changing people's expectations about their relationships with governments.

The challenge is not limited to the introduction of digital technologies into public administrations; but also to integrate their use into public sector modernization efforts.

Similar to other sectors, the decision to use technology for public governance requires coherent and strategic planning of policies for the availability of digital technologies in all areas and at all levels of public administration as well as the framework whereby digital skills can be enhanced across the population. Policy makers and regulators should work together to ensure people have access to technologies, have the digital skills to use them, and that there is trust in using e-government services.⁹

Collaborative efforts should lead to strategies to create an enabling environment, including appropriate legal and institutional frameworks, capacity-development for digital media literacy for citizens and a seamless integration of online and offline features for public participation.

What can policy makers do to spur effective and more open, innovative and participatory governments? According to a recent OECD study,¹⁰ policy makers should:

- Set strategic digital government objectives;
- Take steps to address existing "digital divides" and the need to avoid "new digital exclusions"; as well as the creation of a data-driven culture that enables open data for transparency, better service delivery and public participation;
- Ensure the coherent use of technology across policy areas and levels of government;
- Establish organizational and governance frameworks for effective co-ordination and integration of efforts to produce better policy outcomes and services;
- Strengthen capacities to support better implementation of digital government strategies;
- Monitor results of outcomes.

Governments should also adopt clear business cases for the use of resources on identified objectives. The necessary capacities, including regulatory and legal frameworks, need to be put in place to not only capture new digital government opportunities but also to mitigate associated risks (such as security and privacy).

⁸ http://www.finance.gov.au/policy-guides-procurement/ict_strategy_2012_2015/

⁹ <http://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf>

¹⁰ <http://www.oecd.org/gov/digital-government/recommendation-on-digital-government-strategies.htm>

2.2.2 Agriculture and ICTs

The Role of National e-Agriculture Strategies

“ National e-Agriculture strategies could offer critical support to rationale the use of resources (financial and human), to better harness ICT opportunities and to address challenges in the agricultural sector. The existence of a comprehensive national e-Agriculture strategy could prevent e-agriculture projects from being implemented in isolation and increase efficiency gains from intra-sector and cross- sector synergies. “

Source: Towards National e-Agriculture Strategies, September 2015, available at: http://www.e-agriculture.org/sites/default/files/uploads/kb/2015/09/policy_brief_e_ag_strategies_sept_2015_0.pdf

Using telecommunication/ICTs to enhance agriculture around the world offers a great opportunity for economic growth and poverty alleviation. Universal access and service programmes, especially for broadband access, can overlap with e-agriculture strategies since they can be used to provide remote populations with ICTs, thus helping to reduce poverty.

“Smart Agriculture” measures and programmes can guide farmers when to plant, fertilize and harvest, based on site-specific weather data, thus improving productivity and efficiency. ICT-enabled systems can help create and spread agricultural knowledge, disseminate up-to-date technology, facilitate training programmes, and connect rural businesses to markets.

However, for this opportunity to materialize, e-agriculture projects should be coordinated and sustainability defined. E-agriculture should be part of a clear and collaborative strategy, with synergies with other sectors and linkages between parallel initiatives defined. ICT development and strategic alliance, including with the financial sector, is key to such thinking.

2.2.3 Education and ICTS

National School Connectivity Plans

Policy goals regarding digital inclusion need to be translated into a practical plan and concrete action points for connecting schools. Developing a plan is critical to bringing a strategy from the conceptual stage to the practical level. A plan should address who is in charge of coordination and implementation, how to identify the schools that will be connected, funding sources, technologies to be used, and how the connectivity will be sustained. A plan also can align education sector targets with national ICT goals. And it can promote mechanisms to involve all key stakeholders.

Source: <http://connectaschool.org/itu-module/21/536/en/schools/connectivity/reg/3.1/>

ICTs contribute to making education more accessible and more universally and equitably available to people around the world. They also enable more efficient delivery of quality teaching, more effective learning, and better educational management, governance and administration.

Many countries are realizing the importance of connecting schools and universities, and research institutes to the Internet and have developed e-learning and m-learning strategies for connecting students and researchers. Educators are also increasingly integrating ICTs in their design of learning materials as well as educational methods.

Connectivity provides many educational benefits including access to information, opportunities for collaboration and digital skills, including in the use of technology and online applications. The benefits are particularly attractive for remote schools where Internet access provides the opportunity for online learning and access to educational content.

Alongside investment in technology, there is a need for governments to define and plan how to invest in capacity building in multidisciplinary digital skills and knowledge.

Although many of the benefits identified are only achievable through broadband connectivity, a myriad of technologies can be used for simpler systems and still create value for users. All forms of connectivity, including fixed and mobile broadband as well as satellite broadband contribute to the goal of providing universal education to all.

2.2.4 Health and ICTS

National e Health Strategies

Establishing the main directions as well as planning the detailed steps needed are key to achieving longer-term goals such as health sector efficiency, reform or more fundamental transformation. Ministries of health play a pivotal role, not only in meeting people's needs for care and protecting public health, but in preserving health systems through uncertain times. Ministries of information technology and telecommunications are key to development in all spheres, and can make a vital contribution to the health sector. Common goals and a predictable ICT environment enable coordinated action: building consensus on policy, facilitating better use of shared resources and involvement of the private sector, and investment in skills and infrastructure to improve health outcomes.¹¹

The World Health Organization defines e-Health as "the cost-effective and secure use of ICTs in support of health and health-related fields, including health-care services, health surveillance, health literature, and health education, knowledge and research...".¹²

In order to effectively leverage telecommunications/ICTs for health, regulators and policy makers need to identify strategic and integrated action at the national level. This will allow existing capacity to be used in both sectors while creating the enabling environment for investment and innovation.

2.2.5 Energy and ICTs

ICTs for Energy

Governments have recognized that ICTs are an important part of their strategies for tackling environmental problems.

The incorporation of ICT-enabled solutions and methodologies across the sectors has enhanced energy efficiency and reduced cost. ICTs also have the potential to play a critical role in addressing challenges related to climate change, including by reducing emissions and the carbon footprint. On the other hand, the steadily increasing use of ICTs and their need for energy and impact on the use of energy is also an important factor to consider when defining policies and regulation.

Regulators and policy makers have adopted a range of ICT and environment policies. Green ICT measures, smart grids are some of the topics under consideration.

More still needs to be done to develop and enhance environmental performance along the ICT value chain and to promote ICT applications that can improve and enhance the use of ICTs across the sectors and make them more resource efficient.

ICT applications and systems can lead to higher levels of economic productivity and energy savings. ICTs also consume energy.

¹¹ <http://www.itu.int/en/ITU-D/ICT-Applications/eHEALTH/Pages/NeHSToolkit.aspx>

¹² Resolution 58/28 of the World Health Assembly, Geneva, 2005

With the growing availability of broadband, electricity consumption of households is increasing. Data centres, too, are large energy consumers.

In the European Union, a Code of Conduct has been created in response to increasing energy consumption in data centres to inform and stimulate data centre operators and owners by improving understanding of energy demand within the data centre, raising awareness, and recommending energy efficient best practice and targets. The aim of this Code is to reduce energy consumption in a cost-effective manner without hampering the mission critical function of data centres.¹³

ICTs have allowed us to measure, share, and control our energy usage and patterns.

- Smart manufacturing, for example, using sensor and information networks to monitor energy and optimize systems can achieve efficiency and thus increase productivity.
- Smart grids - electricity grids that use ICTs to gather and act on information from suppliers and consumers in an automated way - deliver electricity more cost-effectively and with lower greenhouse gas emissions. Thorough smart grids, energy from intermittent renewable sources can be used to distribute power much more efficiently.
- Smart “transport” can reduce pollution.

2.2.6 Digital Financial Services

Digital Financial Inclusion

The Consultative Group to Assist the Poor (CGAP) defines digital financial services as “financial services that are offered through digital channels”.¹⁴

“Digital financial inclusion” is defined as “digital access to and use of formal financial services by excluded and underserved populations. Such services should be suited to the customers’ needs and delivered responsibly, at a cost both affordable to customers and sustainable for providers.”¹⁵

Today, 2 billion adults have no access to basic financial services, which represents a barrier to reducing poverty and boosting socio-economic development, in particular for developing countries. But with more than 7 billion mobile cellular subscriptions worldwide, access to, and use of ICTs and other innovative technologies provide a promising way to increase access to financial services to the “unbanked”.

A major component in the digital financial service ecosystem consists of mobile phones and point-of-sale devices which can improve and increase the availability of and delivery of basic financial services to the poor. Stakeholders include banks, microfinance institutions, mobile operators, networks of small-scale agents, as well as other providers. CGAP identifies four categories:

- A full-service bank offering a “basic” or “simplified” transactional account for payments, transfers, and value storage via mobile device or payment card plus point-of-sale (POS) terminal;
- a limited-service niche bank offering such an account via mobile device or payment card plus POS terminal;
- a mobile network operator (MNO) e-money issuer; and
- a nonbank non-MNO e-money issuer.¹⁶

¹³ <http://iet.jrc.ec.europa.eu/energyefficiency/ict-codes-conduct/data-centres-energy-efficiency>

¹⁴ <http://www.cgap.org/topics/digital-financial-services>

¹⁵ <http://www.cgap.org/publications/digital-financial-inclusion>

¹⁶ <http://www.cgap.org/publications/digital-financial-inclusion>

Recognizing the importance of digital financial services for inclusion, the digital financial inclusion agenda calls upon strengthened collaboration between the financial and telecom/ICT sectors.

The Global Dialogue on Digital Financial Services Paper on Regulating for Financial Inclusion (GDDFI, 2016) recognizes that while access to financial services is a crucial enabler of economic and social development,¹⁷ digital financial services involve a range of technical and market, and thus regulatory, issues relating to the fields of telecommunications, financial and competition. Between telecommunications and financial regulators and competition authorities, many countries have sufficient legal powers that, if coordinated, can address the regulatory and competition concerns that are arising in mobile financial services. They only require the political will of these institutions to collaborate towards a common goal. As a result, sometimes these fields are tightly interlinked, as is the case where network effects in telecommunications markets and in financial markets reinforce one another and prevent competition.

¹⁷ World Bank, 1989, *World Development Report: Financial systems and development*.

3 Overview of ICT and Collaborative Regulatory Frameworks

3.1 Telecommunication/ICT Regulation

3.1.1 Evolution of ICT/Telecommunication Regulation

History shows that, in the past, telecommunication was considered a public service like many other utilities (e.g., water, roads), and as such constituted part of the mandate of the government, with the Ministries of Post, Telegraph and Telecommunications (MPTTs) being responsible for operation and regulation. They were responsible for setting policies and technical standards, certifying equipment, controlling and managing the radio spectrum, allocating and controlling numbers, and managing other resources and assets. It was the government that made investment decisions and set prices. They were both operator, policy maker and regulator. In some cases, operation was carried out by state-owned enterprises that were granted privileges while being regulated by government.

Technology and business models have evolved and this led to policy and governance changes, starting in the 1980s. In the US, Great Britain and Japan, policy makers realized the need for reform and innovation, partly because the role of telecommunication/ICTs in opening economic and social opportunities was starting to be recognized. This became part of multilateral talks and trade deals, and the momentum started to increase, with countries around the world following the trend. State-owned operators began to be privatized and liberalization became a global trend, supported by regional decisions (e.g. in the European Union), and commitments taken at global, regional and bilateral level – in particular within the Framework of the World Trade Organization.¹⁸

WTO and Telecommunication liberalization

Commitments in telecommunications services were first made during the Uruguay Round (1986-94), which gave momentum to the liberalization of telecommunications services around the world. Commitments in this first round mainly related to value-added services. In post-Uruguay Round negotiations (1994-97), WTO members went further and negotiated on basic telecommunications services. Since then, commitments have been made by new members, upon accession to the WTO, or unilaterally at any time. In addition, WTO members also committed to a number of regulatory principles as contained in the “Reference Paper”, a blueprint for sector reform that largely reflects “best practice” in telecoms regulation.

> [List of all current telecommunications commitments and exemptions](#)

At the Hong Kong Ministerial Conference (December 2005), a new sector-specific negotiating mechanism was mandated by the trade ministers. Negotiating objectives outlined by WTO members in the Chairman's note to the Trade Negotiations Committee include:

- achieving broad coverage in a technology-neutral manner and significant commitments in all modes of supply
- working with least-developed countries and developing countries to find ways to encourage new and improved offers and to provide technical assistance to support this process
- reducing or eliminating exclusive rights, economic needs tests (i.e. a test using economic criteria to decide whether the entry into the market of a new foreign firm is warranted), restrictions on the types of legal entity permitted, and limitations on foreign equity

¹⁸ https://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_e.htm

- commitment to all provisions of the telecommunications Reference Paper
- the elimination of exemptions to most-favoured nation (MFN) treatment (i.e. non-discrimination).

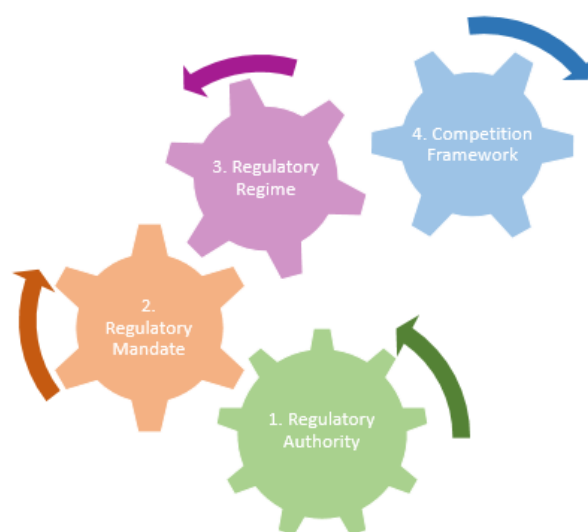
Source: WTO

In some countries, liberalization of certain networks and services was introduced at the same time as privatization, while in others this was a second phase of the reform process. Transition to competitive markets was in many cases introduced in stages with incumbent operators being granted exclusivity periods, often for economic and social reasons and to allow the incumbent to restructure. The next phase of liberalization occurred once the incumbent operator's exclusivity period ended, which led to greater competition in many markets.

The process of privatization and the introduction of competition led to a new governance model, or the 2nd Generation Regulation, according to ITU. Once operation and regulation were separated, and given that many governments still retained some form of ownership of incumbents, independent regulatory authorities were created to oversee and create enabling environments in which effective competition could thrive. These newly created independent entities initially focused on opening the formerly monopolistic markets to competition. Their efforts often related to market entry, consumer protection and interconnection between the new entrants and with the incumbent, as well as access, particularly in areas that were not commercially attractive. Regulators also created processes and procedures in relation to their own functioning, their relationship with other entities directly involved in telecommunication/ICT related issues (e.g., competition authorities, consumer protection agencies, spectrum management agencies) as well as in relation to the oversight of the newly competitive markets (e.g., dispute resolution, sanctions and enforcement, consumer complaints and stakeholder consultation).

Once open markets with fully competitive environments came into being, the role of the independent regulatory authorities evolved from one that focused mainly on ensuring that competition could be introduced to one where regulators focused on fostering an enabling environment for telecommunication/ICT development, addressing in particular market failures. Key to this evolution was the clear definition of the institutional framework, the regulatory mandate, the regulatory regime as well as the competition framework. This is the 3rd Generation Regulation, according to the ITU classification.

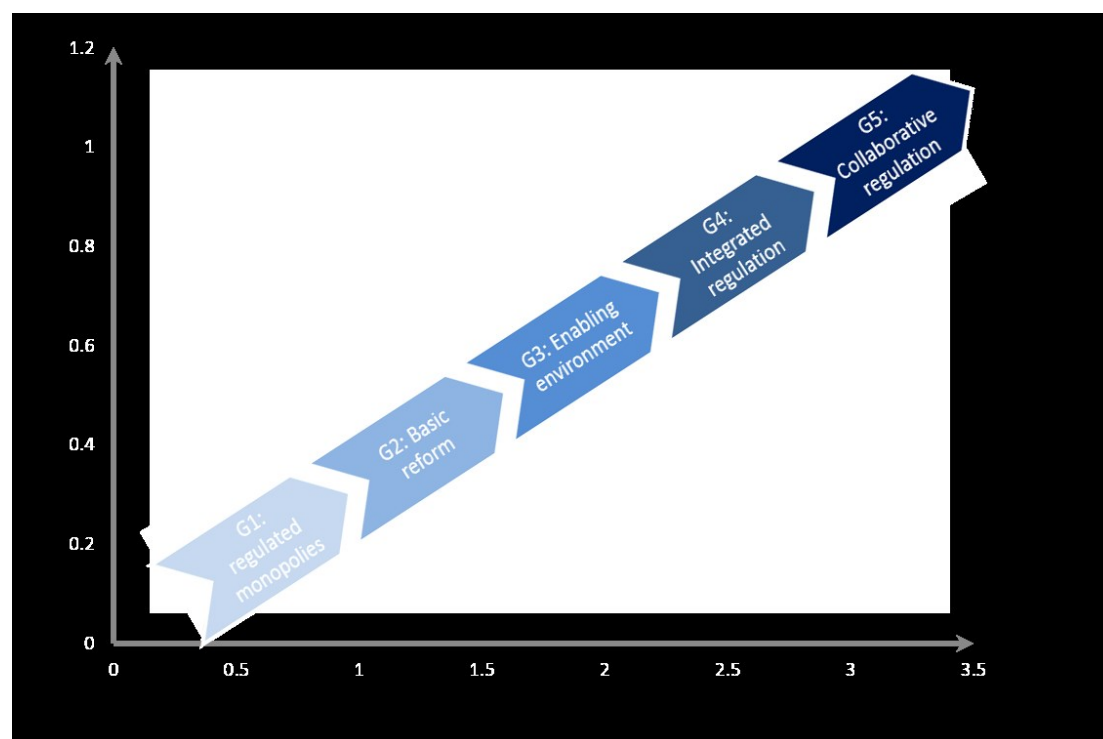
Figure 1: Building Blocks for an Enabling 4th Generation Regulatory Environment



Source: ITU

Greater complexity and a cross-sectoral view, addressing the interaction of the ICT sector to stimulate growth in the broader digital economy has challenged telecommunication/ICT regulators and policy makers. They need to continuously review, adapt and anticipate changes to ensure that their national ICT legal and regulatory framework address how ICTs can help achieve economic and social development goals. This is the 4th Generation Regulation.

Figure 2: Evolution of Regulation



Source: ITU

ITU distinguishes between:

‘1G’ or monopolistic regulation without an independent regulator;

‘2G’ regulation, including the creation of separate regulatory bodies that introduced basic reforms, partial liberalization and privatization across the layers;

‘3G’ regulation with regulators enabling investment, innovation and access, with focus on stimulating competition, and

‘4G’ regulation, with an evolving role of the regulator as a partner for development and social inclusion, focusing on economic and social policy goals through ICT policy and regulation.¹⁹

‘5G’ regulation, with the need to define the foundation, platforms and mechanisms for collaborative regulation with other sectors to help achieve the Sustainable Development Goals.

Today, the smart connected society presents regulators and policy makers with a complex networked environment – locally and globally - where collaboration between sectors is key to the success of smart connected societies. The interconnected nature of digital societies across the sectors means that there is a need for collaboration between government and industry operators, as

¹⁹ ITU Trends in telecommunication Reform, 2015.

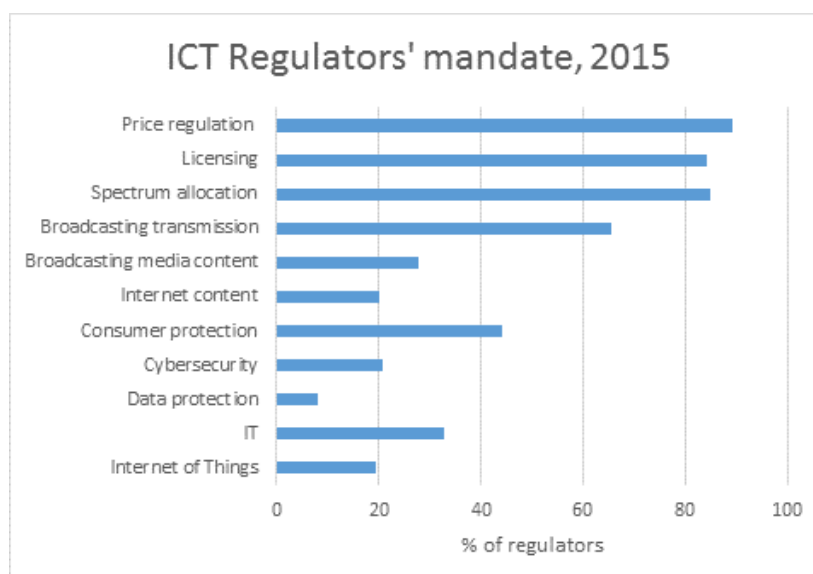
well as between regulators across the sectors to provide effective responses to issues arising in networked communication flows. Today, regulators and policy makers are starting to define the foundation as well as the platforms and mechanisms for collaborative regulation with other sectors such as health, finance, education, energy. Their goal is to define common measures to include and empower citizens so that they can benefit from the opportunities offered by a digital connected society. This is the 5th generation regulation, according to ITU.

3.1.2 Mandate of ICT/Telecommunication Regulators

Today, independent regulatory authorities generally have the responsibility for implementing and administering the regulatory framework, with government ministries responsible for policy-making. Given the widened scope of ICT/telecommunication, policymaking and regulation on issues of relevance to the sector can reside with one ministry or be divided between several government ministries and with one ICT/telecommunications regulator or several (data protection agency, competition authority, spectrum agency, etc.).

In a competitive ICT/telecommunication environment, the mandate of telecommunications regulators generally includes the authority to conduct rulemakings and issue regulations, address various telecommunications issues, including universal service, licensing, interconnection, price regulation, numbering, and spectrum management. Most often, such regulators can also undertake adjudication, sanctions and enforcement. In addition, there are regulatory and policy issues related to technologies and their related services, including spam and consumer concerns regarding privacy, emergency services and quality of service. The range and scope of powers depends on the delegation of powers to such regulators.

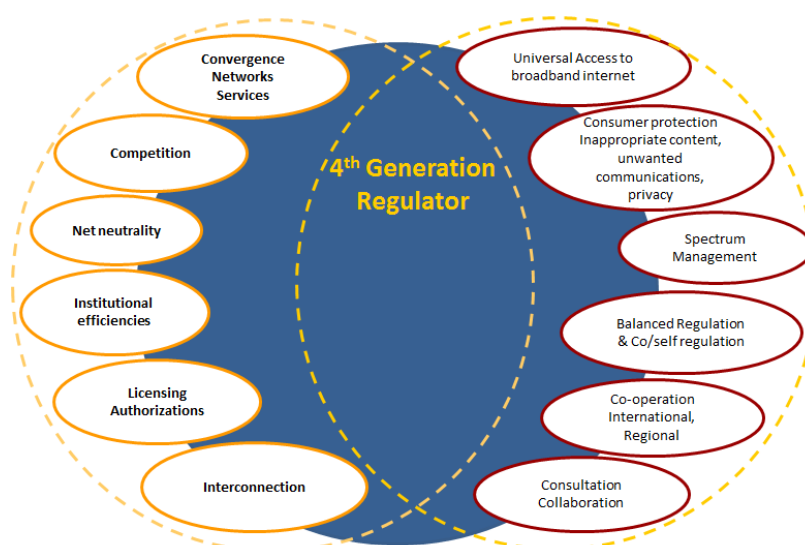
Figure 3: ICT Regulator's Mandate



Source: ITU ICT Eye.

From a first generation of regulators with highly regulated state-owned monopolies, to a second wave of privatizations, opening up of markets and the creation of separate regulatory bodies, to a third phase with focus on competition and the expansion of mandates, the fourth generation of regulators requires adaptability to an industry that is going through innovation. This has affected the mandate of ICT/telecommunication regulators. An overview of issues addressed by 4th generation regulators is shown in the figure below.

Figure 4: 4th Generation Regulation Issues



Source: ITU

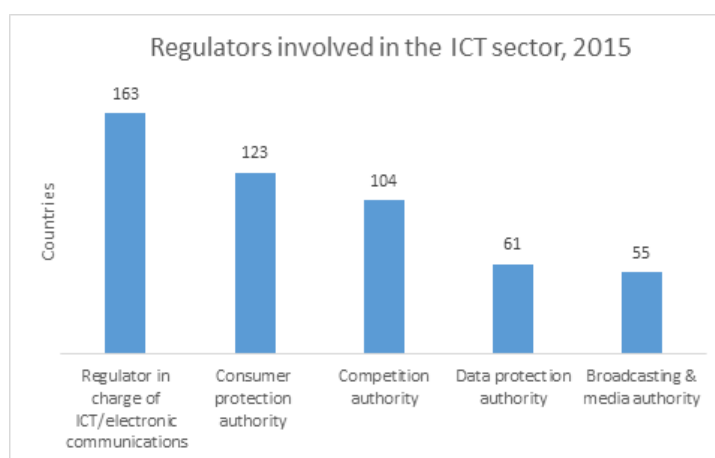
3.2 Interaction with Other Authorities involved in ICT

Regulators increasingly require collaborative strategies with other agencies to develop targeted responses to common challenges and opportunities. Experience shows that coordination with the respective competent authorities and other interested stakeholders is taking place, to create awareness and foster an innovation-and consumer-friendly environment.

There has sometimes been convergence between entities, particularly when there is significant overlap in the markets they cover. The creation of a converged regulator avoids having separate regulators overlapping, thus enabling better efficiencies for both the private and public sectors. Where the mandate is clearly specified and sufficient resources are dedicated to effective regulation, the combination of expertise generally also allows such regulators to effectively address issues relating to new emerging technologies, and to deal with issues such as telecommunication and/or media and broadcasting licensing issues where new models of delivery are replacing old ones.

The lines between services and technology are becoming blurred and examples such as over-the-top ("OTT") and machine-to-machine ("M2M") services have impacted regulatory models.

Figure 5: Regulators Involved in the ICT Sector



Source: ITU ICT Eye & ITU research.

3.2.1 Broadcasting and Media Authorities

New technologies and developments in ICTs have affected telecommunications broadcasting, and the Internet, leading to closer coordination between these sectors. The relative policy and regulatory measures have also converged, including on issues relating to content, intellectual property, and privacy.

Converging ICT/telecommunications regulators with broadcasting regulators is a trend that emerged from the blurring lines between technology and media, as well as from changes in the way that service providers deliver content and bundle services, and users are consuming services and content.

In some countries, this has led to the creation of communications authorities that include telecommunication, media and broadcasting.

Examples of Converged Telecommunication's and Broadcasting Regulators from around the world:

Ofcom is the communications regulator in the **UK** and regulates the TV, radio and video on demand sectors, fixed line telecoms, mobiles, postal services, plus the airwaves over which wireless devices operate. The stated mission of Ofcom is to make sure that people in the UK get the best from their communications services and are protected from scams and fraudulent practices, while ensuring that competition can thrive.²⁰ Ofcom also has the powers to enforce competition law in those sectors for which it is responsible, alongside the Competition and Markets Authority. Ofcom is funded by fees from industry for regulating broadcasting and communications networks, and grant-in-aid from the Government.

The Communication Regulatory Agency (**RAK**) of Bosnia Herzegovina, established in 2001, merged the Independent Media Commission (broadcasting) and the Telecommunications Regulatory Agency (telecommunications). Adopting a convergent approach, RAK's mandate includes telecommunications, radio, broadcasting (including cable television) and associated services and facilities.²¹

As part of the Constitutional Reform of 2013 in **Mexico**, the Federal Telecommunications and Broadcasting Law was published on 14 July 2013, and established a new regulatory framework in the telecommunications and broadcasting. The object of the Law is to regulate: the radio-electric spectrum, the public telecommunication networks, the access to active and passive infrastructure, orbital resources, satellite communication, the provision of public services of general interest of telecommunications and broadcasting and the convergence between both services, the rights of the users and audiences, and (the process of competition and free market participation in these sectors. The Federal Institute of Telecommunications (the IFT), created by the Constitutional Reform as an autonomous constitutional body, is responsible for the regulation, promotion, and supervision of the use, approval, and exploitation of: the radio-electric spectrum, orbital resources, satellite services, the public telecommunications networks, broadcasting and telecommunications services, the access to active and passive infrastructure, and other essential facilities.²²

The Telecommunications Authority of **Trinidad and Tobago** is the independent regulatory body responsible for regulating both telecommunications and broadcasting sectors, managing spectrum and number resources, establishing equipment and service quality standards, setting guidelines to

²⁰ <http://www.ofcom.org.uk/about/what-is-ofcom/>

²¹ <http://rak.ba/eng/>

²² <http://www.ift.org.mx/>

prevent anti-competitive practices and encouraging investment in order to facilitate the availability of affordable telecommunications and broadcasting services to all.²³

In **Namibia**, CRAN is the Communications Regulatory Authority of Namibia. CRAN regulates telecommunication services and networks, broadcasting services, postal services and the use and allocation of radio spectrum.

The Independent Communications Authority of **South Africa** (ICASA) is the regulator for the South African communications, broadcasting and postal services sector. ICASA was established by an Act of statute, the Independent Communications Authority of South Africa Act of 2000, as Amended. ICASA's mandate is spelled out in the Electronic Communications Act for the licensing and regulation of electronic communications and broadcasting services, and by the Postal Services Act for the regulation of the postal sector.²⁴

In **Australia**, the ACMA is responsible for regulating online content, including Internet and mobile phone content, and enforcing Australia's anti-spam law. The ACMA's responsibilities include:

- promoting self-regulation and competition in the communications industry, while protecting consumers and other users
- fostering an environment in which electronic media respect community standards and respond to audience and user needs
- managing access to the radiofrequency spectrum
- representing Australia's communications interests internationally.²⁵

In **Singapore**, the Infocomm Media Masterplan 2025 (2015), recognizes that convergence is accelerating, as demonstrated by traditional telecommunications providers entering the media business, and by social media players entering the telecommunications market. As a result of this Plan, the merger of the Info-communications Development Authority (IDA) and the Media Development Authority (MDA) was announced in 2016 with the aim of streamlining of the legislative and licensing framework governing communications and media players. The new Info-communications Media Development Authority of Singapore (IMDA) will develop and regulate both the information and communications and media sectors, as a converged regulator. The Personal Data Protection Commission (PDPC), the regulator for the Personal Data Protection Act (PDPA), will also be part of the new IMDA. Various pieces of legislation will be amended and promulgated, including the Broadcasting Act (Cap. 28), Films Act (Cap. 107) and Telecommunications Act (Cap. 323).²⁶

3.2.2 Competition authorities

The introduction of competition and liberalization of ICT/telecommunication markets led to collaboration between the newly created telecommunication regulatory authorities and competition authorities. Although, as discussed in the ITU-*infoDev* ICT Regulation Toolkit²⁷, in many countries, the telecommunications regulator was often responsible for technical regulation such as spectrum allocation, number allocation, type approval, and standard setting, telecommunications-specific economic and social regulation such as licensing, universal service, price regulation, access and

²³ <https://tatt.org.tt/AboutTATT.aspx>

²⁴ <https://www.icasa.org.za/>

²⁵ <http://www.acma.gov.au/theACMA/About/Corporate/Responsibilities/regulating-media-communications-acma>

²⁶ <http://www.lexology.com/library/detail.aspx?q=f10c8f3f-c6e0-4ac9-9c65-1de46c22bd1f>

²⁷ <http://www.ictregulationtoolkit.org/6.5>

interconnection, and rights-of-way were also often part of the telecommunication regulator's mandate.

Competition authorities, on the other hand, are generally mandated with tasks relating to anti-competitive behaviour and mergers with the aim of avoiding collusion and controlling the ability of market players to restrict competition. They also generally seek to protect consumers from anti-competitive practices.

In practice, however, there is some overlap between the issues that the telecommunications regulatory authority and the competition authorities address, for example in relation to significant market power or pricing policies, which raises the question of whether competition aspects relating to telecommunications regulation should be integrated into the broader powers and responsibilities of the competition authority and removed from the sector regulator, or whether both agencies should collaborate on competition issues.

Where there is shared responsibility relating to competition issues, collaboration needs to be organized and managed. A key element to ensure successful collaboration related to the clear definition of the role and mandate of each institution. This avoids duplication, legal uncertainty and disputes or unclear decision-making.

Collaboration with Competition Authorities

Telecommunication regulators can contribute to the work of the competition authority by:

- designing *ex-ante* rules that will support the competition authority's goals and facilitate its role as a watchdog.
- sharing its sector expertise with the competition authority for example in the case of mergers or anticompetitive conduct, or when evaluating market structures
- enforcing the competition authority's rulings

Source: <http://regulationbodyofknowledge.org/fag/market-structure/competition-authorities-what-are-the-potential-functions-of-competition-authorities-and-how-can-they-collaborate-with-sector-regulators/>

3.2.3 Consumer Protection Agencies

Consumer protection is a key element of an effective competitive market.

Although in many cases ICT/telecommunication regulators have some form of consumer protection responsibilities in their mandate, consumer organizations and associations often exist in parallel – albeit that in many cases their mandate is wider than just telecommunications/ICTs. Such organizations, however, have a role to play in identifying consumer protection issues, providing data and carrying out surveys in relation to, for example, tariffs and quality of service.

To benefit from competition and be able to make informed choices, however, consumers need to be well informed, not just about price, but also on the qualitative aspects of the service. An important element of consumer empowerment is the need to provide the mechanisms whereby consumers are also educated on the rights that they have and how to exercise those rights. It is not just sufficient to publish the information, but awareness raising and education on consumer rights is also core to a competitive market.

ICT/Telecommunication policy and regulation relating to consumer protection and empowerment has generally focused on creating mechanisms to ensure consumers are informed about their rights and choices as well as to the quality of service provided in the ICT/telecommunication market, that they are protected from the unfair practices of the companies providing ICT/telecommunications services, and that they have the right to redress where issues occur.

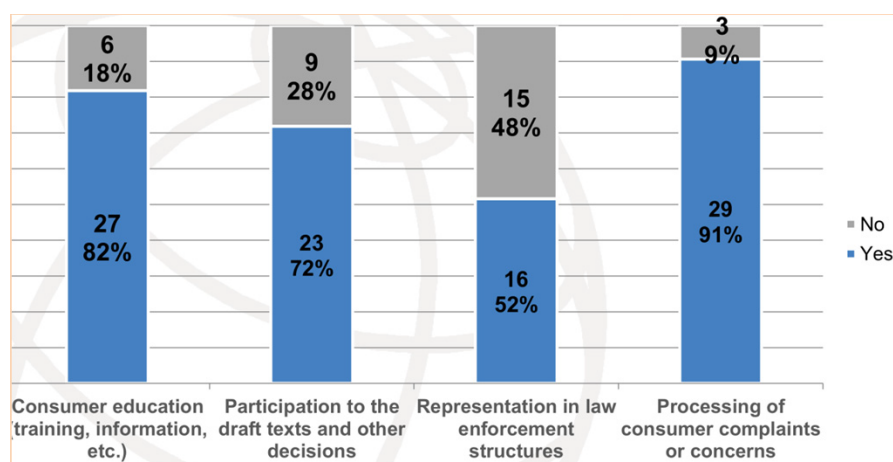
Regulatory tools and measures to protect consumers include regulations on misleading conduct, disclosure requirements, product regulation, and regulation aimed at allowing consumers to conveniently switch between suppliers in the telecommunications industry. Access and interconnection as well as interoperability standards and number portability are also aimed at providing consumers with choice and reliable communication tools.

Concerning the protection of their rights, measures such as the creation of industry codes for consumers, the creation of consumer ombudsmen, data privacy and protection measures as well as the collection and publication of comparative data for consumers are also key.

Redress is also important, with consumers needing meaningful and affordable access to fair, easy-to-use, transparent and effective mechanisms to resolve domestic and cross-border disputes in a timely manner and obtain redress, as appropriate, without incurring unnecessary cost or burden.

OECD identifies mechanisms such as internal complaints handling and alternative dispute resolution as well as small claims tribunals, ombudsmen, and complaints systems (which provide feedback to regulators and suppliers) as important institutions for consumers in many markets in addition to regular tribunals²⁸. They are cheaper, quicker, and provide a pro-active forum for the resolution of disputes such as for example, consumer complaints about the billing process. Out-of-court redress mechanisms should not, however, prevent consumers from pursuing other forms of dispute resolution and redress.

Figure 6: ICT/Telecom related responsibilities of consumer protection agencies



Source: ITU

3.2.4 Data Protection Agencies

With regard to areas like privacy and data security, the competences of ICT/telecommunication regulatory authorities vary amongst countries, with some having only limited or no competences at all. The right to privacy has been a long established principle in many countries, enshrined in laws and often even in the Constitution. Today, many countries have introduced personal data privacy legalization that goes beyond consumer protection. The question in a digital connected society is how to apply these principles and who carries the mandate for regulation and enforcement.

New laws, regulations and codes of practice must aim to balance the interests of individuals who have a right to privacy with the social benefits of a growing digital economy and public safety concerns. In an interconnected world anything online can be located anywhere on the planet, and

²⁸ OECD Recommendation on Consumer Dispute Resolution and Redress, OECD 2007, available at: <https://www.oecd.org/sti/consumer/38960101.pdf>

with the rise of cloud computing anything online can, in principle, be transferred anywhere at any time. The result is that measures are being defined in relation to the data ‘controller’ of information, the data ‘processor’, and individuals. For individuals, the concept of “informed consent” means that for individuals, the right to opt in or opt out and measures relating to the retention of data are now at the core of discussions.

In the European Union, regulations have been defined regarding the privacy and confidentiality of user information that apply directly to electronic communications companies (telecommunications companies and internet services providers) and to any entity using such communications and electronic communications networks to communicate with customers, e.g. by telephone, via a website or over email.²⁹

This is also the case in other countries and regions. As of April 2016, some 108 countries had implemented national privacy or data protection laws.³⁰ In Australia, for example, privacy provisions in telecommunications legislation and in other related legislation have been harmonized, this with the aim of to ensure a consistent standard of privacy protection applied to both the public and private sectors.

In terms of enforcement of such legislation, there is often a shared responsibility between data protection authorities and ICT/Telecommunication regulators or even policy makers. In Finland, for example, the Office of the Data Protection Ombudsman is an independent authority operating in connection with the Ministry of Justice. The office is run by the Data Protection Ombudsman, appointed by the Council of State for a term of five years. FICORA, the Finnish Communications Regulatory Authority, on the other hand, supervises the data protection of electronic communications in the operations of telecommunications operators, corporates or associations, and, since 2015, also in other communications providers' operations. The supervision also concerns, on certain conditions, services provided from abroad. FICORA supervises that telecommunications operators implement their network and communications services in an information secure-manner so that the confidentiality of the communications is not endangered. FICORA also oversees compliance with the Information Society Code and other provisions and regulations issued under it. FICORA is also in charge of processing of identification data, protection of communications and decoding, and compliance with the provisions on the information service of communications services.³¹

In the United States, the Federal Trade Commission (FTC) has overall responsibility of supervising the enforcement of federal requirements on different sectors of the economy. FTC is responsible for supervising whether information is collected and used about customers by telecom companies, confidentiality of health records, Inland Revenue data, etc., and to generally apply consumer protection regulations.³²

There are also global initiatives such as the Global Privacy Enforcement Network³³ started in 2010 following the adoption in 2007 by the OECD Council of the *Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy* which provided that

“[m]ember countries should foster the establishment of an informal network of Privacy Enforcement Authorities and other appropriate stakeholders to discuss the practical aspects of privacy law

²⁹ BEREC Report on IoT – available at:

[http://berec.europa.eu/files/document_register_store/2016/2/BoR_\(16\)_39_BEREC_IoT_Report_FINAL_for_publication.pdf](http://berec.europa.eu/files/document_register_store/2016/2/BoR_(16)_39_BEREC_IoT_Report_FINAL_for_publication.pdf)

³⁰ UNCTAD Cyberlaw Tracker 2016

³¹ <https://www.viestintavirasto.fi/en/steeringandsupervision/dataprotection.html>

³² <http://broadbandtoolkit.org/3.9>

³³ <https://www.privacyenforcement.net/>

enforcement co-operation, share best practices in addressing cross-border challenges, work to develop shared enforcement priorities, and support joint enforcement initiatives and awareness raising campaigns.”³⁴

3.4 Multisector Regulators

Some countries have established multisector regulators as a way of regulating utilities and sometimes have included other sectors. This is an example of collaborative regulation.

Advantages, in addition for providing the institutional and legal framework for collaboration and the context to leverage ICTs in other sectors, include:

- Uniform regulatory strategy and similar approaches in all regulated sectors;
- Similar procedures in dealing with customer complaints, supervision of utilities;
- Ability to apply experience from one sector to other sector and to leverage expertise and resources across the sectors.³⁵

In Eastern Europe, examples of Multisector Regulators include the Public Utilities Commission (PUC) of Latvia, the Energy and Public Utility Regulatory Authority of Hungary, and the Agency for Communication Networks and Services of the Republic of Slovenia. PUC in Latvia is mandated with regulatory functions in relation to energy, electronic communications, post, railway transport, waste disposal and water management.³⁶ The Agency for Communication Networks and Services of the Republic of Slovenia, for example, regulates and supervises electronic communications, as well as the radio frequency spectrum and broadcasting. In addition, its mandate includes the regulation and supervision of the postal and railway service markets.³⁷

Created in 2005, the *Bundesnetzagentur* (Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway) was created in Germany as a separate higher federal authority to bring together various sectors and agencies. The Agency works within the scope of business of the Federal Ministry of Economics and Energy. It also acts as the root certification authority under the Electronic Signatures Act³⁸ The Multi-sector regulator in Germany was built up gradually by adding further responsibilities to RegTP, and the change of names in 2005 to *Bundesnetzagentur*. Interesting to note, however, is that the Cartel office (BKartA) remains responsible for competition law intervention. Although there are no concurrent powers between both agencies, meaning that there is no application of general competition law by BNetzA, elements of the general competition law are directly incorporated as provisions in the Telecommunications Act and the Energy Industry Act. The relevant laws however provide for information exchange to ensure legal certainty and avoid duplication or uncertainty.³⁹

In the Bahamas, prior to the sector reform process launched in 2009, the task of regulating electronic communications was shared between a number of authorities including the Public Utilities

³⁴ <https://www.oecd.org/sti/ieconomy/38770483.pdf>

³⁵ PUC (2011), www.sprk.gov.lv/uploads/doc/Multiregulator.pdf

³⁶ [http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=GOV/RPC/NER\(2014\)6&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=GOV/RPC/NER(2014)6&docLanguage=En)

³⁷ <http://www.akos-rs.si/about-akos>

³⁸ http://www.bundesnetzagentur.de/cln_1432/EN/General/Bundesnetzagentur/About/AboutTheBundesnetzagentur_node.html

³⁹ http://www.regulatel.org/wordpress/wp-content/uploads/2015/05/Pro_competitive_electronic_communications_Alemania.pdf

Commission (PUC) and the Television Regulatory Authority (TRA), which were responsible for overseeing the telecommunications and broadcasting sectors, respectively. In 2009, the sector was reformed, and this led to the creation of URCA that was organized as a multi-sector regulator, in charge of the electricity, telecommunications, water and gas sectors, and responsible for promoting the interests of consumers and promoting effective competition.⁴⁰

⁴⁰ <https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2014/Discussion%20papers%20and%20presentations%20-%20GSR14/Case%20Study%20GSR14%20-%20URCA.pdf>

5 Recommendations for Collaboration in a Smart Connected Society

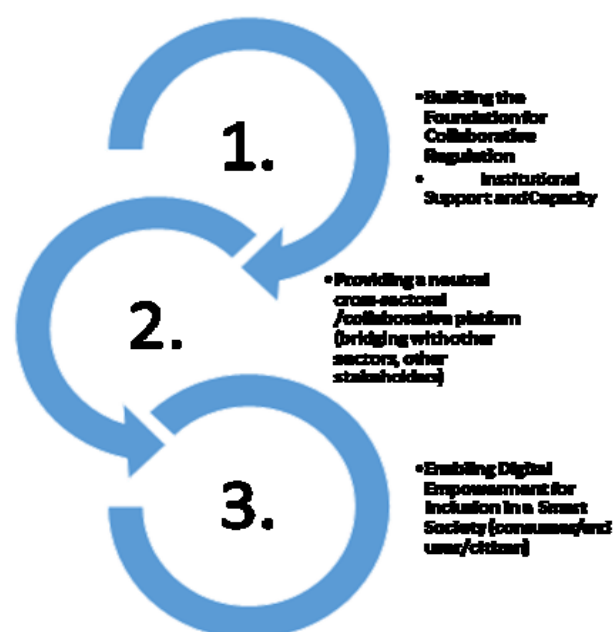
Although policy and regulatory frameworks have evolved independently in many sectors over the past years, recognition has grown that there is an increasing interdependence between sectors. Technology developments are enabling effective global, regional and local development through knowledge management, sharing and collaboration between all sectors and at all levels of government as well as with business and users. There are clear opportunities to empower and include people around the world in a trusted, connected digital society.

Although in most countries, some kind of coordination mechanisms to ensure close and effective dialogue with the different tiers of government involved in regulating ICTs exist, systematic and institutionalised mechanisms for collaborative regulation to leverage ICT/telecommunication in other sectors is still being discussed.

ICT as well as other sector policy makers and regulators are stakeholders in the process of development. This makes transparent, practical cooperation and communication across sectors as well as between regulators and policy-makers as well as with other stakeholders essential to ensuring that regulation is responsive to government policy decisions and the realities of the markets around the world.

5th Generation regulation means having the necessary tools for creating an enabling environment for effective collaboration across the sectors so as to include and empower citizens through ICTs. It also means adopting a holistic view so that ICTs can be leveraged across the sectors. The decision to use technology across the sectors as a tool for economic and social development requires coherent and strategic planning of policies for the availability of digital technologies in all areas and at all levels as well as the framework whereby digital skills can be enhanced across the population. Policy makers and regulators should work together to ensure people have access to technologies, have the digital skills to use them, and that there is trust in using ICTs.

Figure 7: 5th Generation Collaborative Regulation



Source: ITU

Collaborative regulation starts with holding an inclusive dialogue across the sectors to leverage the potential of ICTs/telecommunications for economic and social development, empower, include citizens, and enable them to be an integral part of a connected digital society. Issues to be addressed include the challenges and risks associated with the co-existence of different regulatory frameworks, ways to mitigate risks in fast changing ICT and education, health, banking, administration, energy, broadcasting environments, the need for harmonized regional and international regulations, and the roles of responsible entities.

Options include multisector regulators, but this is not the only option. Countries can also opt for collaboration mechanisms across and between sectors that support separate independent regulatory frameworks of the individual regulators and policy makers. Such collaborative mechanisms should enable regulators and policy makers to work closer together on issues of cross-sectoral significance and to learn lessons across industries which help to improve regulation and the promotion of competition in order to secure better outcomes for consumers.

A call for regulatory collaboration

ITU's Global Symposium for Regulators is a unique, neutral platform where regulators and policy makers have come together every year since 2000 to share their experiences and expertise. Every year, Best Practice Guidelines are adopted. Since 2014, such guidelines have recognized the need for and have called for collaboration among regulators and across the sectors.

Such guidelines have included:

Given the global nature of online services and apps, cross-border harmonization of relevant regulatory policies as well as enhanced collaboration among national government agencies, regional and global organizations is essential for creating a global digital ecosystem while putting in place effective safeguards against fraud and abusive practices.

GSR15 "Best Practice Guidelines to Facilitate the Widespread Adoption and Use of Mobile Applications and Services through Targeted Regulation"

We recognize that, in enforcing and reviewing relevant legislation, regulators and policy makers must establish effective mechanisms for cooperation (such as memoranda of cooperation) with dedicated consumer protection authorities, service providers and other relevant bodies at the national, regional and international level. In doing so, clearly defining roles and responsibilities between the parties is fundamental, as well as information and resources sharing, as appropriate.

GSR14 "Best Practice Guidelines on Consumer Protection in a Digital World"

We believe regulators have a role to play in building consumer trust and protecting security of services by appropriately addressing data protection, privacy issues and cybersecurity matters. It could be done by strengthening cooperation with other government agencies at the national level and by collaborating with other regulators and other partners at the regional and international levels. We are mindful that the exchange of experience, knowledge and ideas is vital in facing the new challenges in an interconnected global borderless digital ecosystem.

GSR13 "Best Practice Guidelines on the Evolving Roles of both Regulation and the Regulators in a Digital Environment"

The creation of a converged regulator in charge of ICTs and broadcasting could be an effective step towards enabling market integration in a converged environment. Should this not be feasible, closer coordination and collaboration between the sector-specific regulatory authorities in charge of telecom, broadcasting and electronic media, as well as authorities in charge of competition is essential.

Strategic and policy activities to build the information society and to play an inter-sectoral coordinating role should be integrated into the converged regulator's mandate.

Close collaboration with other concerned agencies is needed to ensure that appropriate measures and tools are put in place to safeguard Intellectual Property Rights (IPR), Internet safety covering such issues as the protection of the children online and fraudulent activities.

GSR09 “Best Practices Guidelines for innovative regulatory approaches in a converged world to strengthen the foundation of a global Information Society”

ICT/telecommunications regulators can create an enabling collaborative environment by sharing guiding principles and best practices with other sectors and encouraging an inclusive dialogue on issues where ICT/telecommunications may be leveraged in other sectors. Discussions could also seek to identify options and ways to strengthen collaboration, build synergies, and develop collaborative regulatory approaches.

A next step is to define approaches for effective coordination, cooperation and accountability across the sectors, this between government departments, between government departments and regulators, and with relevant non-public actors. Such collaboration mechanisms can contribute to achieving 5th generation regulation and constitutes a fundamental building block for smart societies in a connected world.

Incorporating mechanisms to engage citizens, including disadvantaged and vulnerable groups, is also a key element of collaborative regulation. This requires policies to enhance digital skills and using ICTs to promote engagement.

GSR-16 Discussion paper

EMERGING TECHNOLOGIES AND THE GLOBAL REGULATORY AGENDA

Work in progress, for discussion purposes
Comments are welcome!

Please send your comments on this paper at: gsr@itu.int by 30 May 2016



The views expressed in this paper are those of the author and do not necessarily reflect the opinions of ITU or its Membership.

This paper was prepared by *Kathryn Martin, Kelly O’Keefe and Logan Finucan* from *Access Partnership*.

Contents

1	Executive Summary	4
2	Introduction.....	5
3	Evolving Delivery Platforms	7
3.1	Fifth-generation Mobile Networks (IMT-2020 or 5G)	7
3.1.1	What will IMT-2020 offer?	8
3.1.2	Small Cells	10
3.1.3	Millimeter Waves	10
3.2	Satellite Communications Technologies.....	11
3.2.1	Geostationary High-throughput Satellites	11
3.2.2	NGSO Systems	12
3.2.3	Nanosatellites	13
3.3	High-altitude Platform Stations (HAPS)	15
3.4	Evolving platform stations.....	16
4	Changing Architectures and Complementary Technologies.....	17
4.1	Advances in Network Architectures	17
4.1.1	Cloud Computing.....	17
4.1.2	Cloud-RAN Using Fronthaul	18
4.1.3	Mobile Edge Networking (MEN).....	19
4.1.4	Heterogeneous Networks (HetNets).....	20
4.1.5	Network Slicing.....	20
4.2	Advances in Software	22
4.2.1	Network Function Virtualization (NFV)	22
4.2.2	Cognitive Computing.....	23
4.2.3	Delay-tolerant Networking (DTN).....	24
4.2.4	Self-organizing Networks (SON)	24
4.3	Radio and Antenna Technologies	25
4.3.1	MIMO	25
4.3.2	Beamforming	25
4.3.3	Cognitive Radio system	25
5	Emerging and Evolving Applications.....	28
5.1	Internet of Things (IoT) and Machine to Machine (M2M) – Applications for a Smart Society	28
5.1.1	Smart Cities	30

5.1.2	Smart Manufacturing and the Industrial Internet of Things	31
5.1.3	Intelligent Transportation Systems and Connected Cars	32
5.2	Unmanned Aircraft Systems (UAS)	33
5.3	Healthcare	34
5.4	Geospatial Technology	34
6	Implications for Business Models	36
6.1	Greater Competition to Connect Everything	36
6.2	Established Telecommunications Operators Are Evolving.....	37
6.3	More Companies Are Now “Technology” Companies	38
6.4	More Have a Stake in ICT and Spectrum Management Discussions	39
6.5	New Partnerships Will Emerge to Explore New Opportunities	40
7	Spectrum Management Considerations.....	41
7.1	Evolving Trends	41
7.2	Current Spectrum Management Techniques.....	42
7.3	Spectrum Management Tools.....	43
7.3.1	Flexibility	43
7.3.2	Harmonization	43
7.3.3	Alternatives to Device Licensing	44
7.3.4	Spectrum Sharing	45
8	Considerations and Recommendations for Regulators.....	47
8.1	Using New Technologies to Support Existing Policy Goals.....	47
8.2	Developing Effective Regulatory Approaches	47
8.3	Creating the Environment for Investment and Innovation	48
8.4	Managing Spectrum Resources	48
8.5	Building trust and confidence	49
8.6	Developing Standards.....	49
9	Conclusions.....	50

1 Executive Summary

This report surveys recent developments in technology and explores their implications for telecommunications and spectrum regulators. The ICT community is striving to bring robust connectivity to all corners of the globe, which is helping drive both innovation and ways in which technologies can be used to improve economic and social development. New means of connectivity plus enhanced architectures promise improved coverage, greater capacity, more efficient use of spectrum, and more flexibility for effective delivery of the ICT services. In turn, technological innovations are unlocking new applications, such as those composing the Internet of Things (IoT) and the emerging Smart Society.

The prospect of constant connectivity and complex interconnection of devices is also shaping private-sector business models. Providers of telecommunications services are moving fast, investing in future systems, and exploring new commercial opportunities with other industry sectors as they try to find their place in a new ecosystem that demands flexibility to meet changing demands. Increasingly, new classes of companies (not just those previously thought of as “technology” companies) are developing new capabilities and developing innovative products and services that rely on new connectivity and data services.

These changes are placing increasing demands on spectrum resources, with implications for spectrum management practices. New platforms – principally 5G (IMT-2020) as well as others, such as high altitude platforms (HAPS), or NGSO satellite constellations – will need new spectrum resources in order to reach their full potential. Regulators must be familiar with these evolving technologies, understand their spectrum needs, and ensure that their own spectrum management practices are sufficiently nimble to adapt while protecting existing services.

Regulators will need to ensure that legal and regulatory frameworks are sufficiently flexible. This paper makes a number of recommendations on how they can meet these challenges and best position themselves to unlock the benefits of new technologies for their citizens. These suggestions will help them:

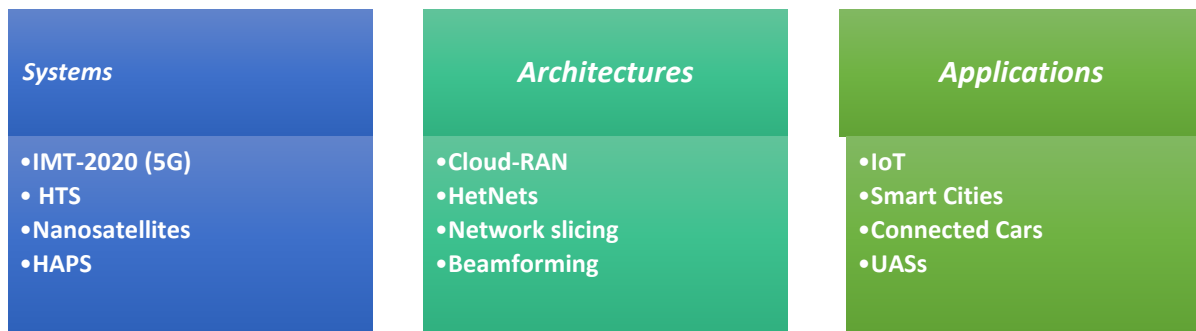
1. harness these technologies to pursue policy goals;
2. develop more effective regulatory approaches;
3. create an environment for growth and innovation;
4. manage limited spectrum resources more productively;
5. build trust and confidence in new technologies;
6. contribute to the development of effective standards.

2 Introduction

Information and communication technologies (ICTs) are the foundation of growth and development in the modern global economy. Many of these technologies rely on spectrum, raising questions of how existing spectrum resources can be efficiently used. How regulators manage spectrum resources and provide an enabling environment to support the development of innovative wireless technologies will be a critical component of the 5th Generation Regulators' toolkit.

Information and communication technologies are advancing in three key areas:

1. New *platforms* for the delivery of broadband and connectivity services are enabling new services and the possibility of being always connected.
2. New network *architectures* and complementary technologies are increasing the capabilities of platforms and Internet-based services.
3. New *applications* of these advances are transforming consumer demand, available services, and private-sector business models.



Due to the crucial importance and regulatory implications of these technological advances and their applications, particularly the roll-out of IMT-2020 (5G), regulators must look ahead to understand these new frontiers, emerging business models, and the regulatory practices that allow innovation to thrive. This paper will help regulators understand these challenges. It proceeds as follows:

Chapter 3 examines evolving platforms, including International Mobile Telecommunication (IMT-2020), the ITU name for future 5G systems, and mobile-based networks, new satellite systems, high-altitude platforms, and other wireless network technologies that will enable new forms of connectivity.

Chapter 4 examines trends toward new network architectures, software advances, and other complementary technologies that increase the flexibility and efficiency of services, such as Cloud-RAN, heterogeneous networks, network function virtualization (NFV), and network slicing.

Chapter 5 examines new applications of these technologies that regulators may expect to grapple with, including the Internet of Things (IoT), unmanned aircraft systems (UAS), intelligent transport systems (ITS), and other applications to infrastructure, manufacturing, and health.

Chapter 6 investigates the implications of these technological changes for private-sector practices, business models, and traces how telecommunications operators are evolving.

Chapter 7 discusses how these new technologies and applications impact spectrum management decisions, and outlines tools regulators have to grapple with them.

Chapter 8 discusses the challenges these advances present to regulators in a number of areas and makes recommendations on how to address them while maximizing the benefits new technology can bring.

3 Evolving Delivery Platforms

Choices in the communications market have been fairly clear and consistent to date. Though technology has changed and capabilities have improved, clear types of platforms have used wireless technologies to offer predictable types of services; terrestrial mobile networks have provided voice communications and high-quality data services, while satellite operators have provided mobile and fixed communications, as well as data services and direct-to-home video. Recent advances in technology are transforming these platforms, the way that they use spectrum and the services they can provide. Traditional players and some new classes of operators are moving quickly to develop new types of services, especially internet based services. Importantly, the development of these platforms is often driven by the need to use spectrum more efficiently while also delivering more capabilities for users who need to always be connected, and also to link those who remain un-connected to the digital economy.

To understand the evolving marketplace, regulators need to understand these changing platforms and their capabilities. The following section will provide an overview of these technologies, including evolving expectations of IMT-2020, which is the ITU's global standard for International Mobile Telecommunication systems (also known as 5G), new geostationary and non-geostationary satellite systems, nanosatellites, and high-altitude platform stations.

3.1 Fifth-generation Mobile Networks (IMT-2020 or 5G)

User demand for data is rapidly rising and will soon surpass the capabilities of current mobile networks. To give an indication of the growth in mobile services, US mobile network operator AT&T reports that they witnessed a 100,000% increase in data traffic in its wireless network from January 2007 through December 2014.¹ This unprecedented growth is expected to continue as demand changes not just in developed markets but as more of the global population becomes connected. Ericsson estimates that over 90% of the world's populations above the age of six will have a mobile phone by 2020.² Beyond 2020, ITU-R (the Radiocommunication Sector of ITU) has estimated that between 2020 and 2030 global International Mobile Telecommunications (IMT) traffic will further increase by a factor of between 10 and 100.³

How will mobile operators keep up with this demand? Many are working hard to develop fifth-generation mobile networks of IMT-2020 systems and expect introduction to begin in 2020. IMT-2020 refers to the next stage of the evolution of mobile communications, following IMT-Advanced (i.e. 4G/LTE). It is more accurately an "ecosystem" than a platform, offering greater data rates and mobility, lower latency, and supporting billions of users/connected devices and multiple applications.

Discussions on IMT-2020 future mobile systems are well underway in ITU as well as in several research bodies and standards organizations around the world. Despite, or perhaps because of, diverse potential approaches to IMT-2020, private-sector companies have already begun to make substantial investments in

¹ "AT&T Adds High-Quality Spectrum to Support Customers' Growing Demand for Mobile Video and High-Speed Internet," AT&T, 30 January 2015, http://about.att.com/story/att_adds_high_quality_spectrum_to_support_growing_demand_for_mobile_video_and_high_speed_internet.html

² Ericsson, *Ericsson Mobility Report*, November 2014, <http://hugin.info/1061/R/1872291/659558.pdf>

³ Report ITU-R M.2370-0 (07/2015): *IMT traffic estimates for the years 2020 to 2030*, <http://www.itu.int/pub/R-REP-M.2370-2015>

order to try to become industry leaders in IMT-2020. SNS Research recently estimated that USD 6 billion will be spent on IMT-2020 research, development, and trial deployments by 2020.⁴

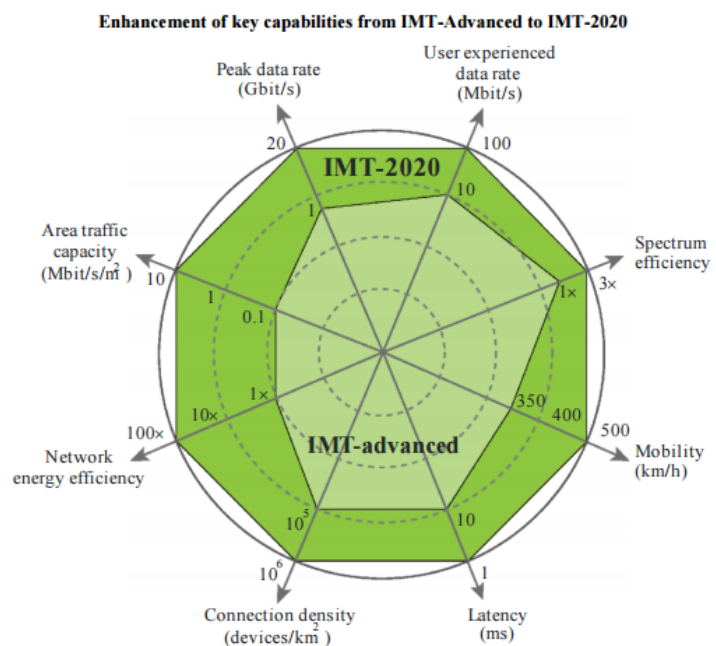
3.1.1 What will IMT-2020 offer?

IMT-2020 is being designed to meet the growing and changing demands of the marketplace for bandwidth and data rates, as well as to support a multitude of application. Some of the expected criteria are:

1. increase in peak data rate and data capacity;
2. massive increase in the number of connections;
3. significant increase in the number of applications supported (for example, the IoT, M2M, gaming, and specialized vertical market support services)
4. decrease in latency;
5. decrease in energy consumption (improvement in energy efficiency);
6. increase in spectrum efficiency;
7. increase in mobility (in terms of speed); and
8. increase in user density.

In September 2015, the Recommendation ITU-R M.2370-0 “*IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*” provided some specific targets for these criteria, measuring IMT-2020 relative to IMT-Advanced.⁵ These include:

- 100 Mb/s user experienced data rates;
- 20 Gb/s peak data rates;
- up to 500 km/h with acceptable QoS;
- 1 ms air interface latency;
- $10^6/\text{km}^2$ connection density;
- 100x better network energy efficiency than IMT-Advanced;
- 3x better spectrum efficiency than IMT-Advanced; and
- 10Mb/s/m^2 area traffic capacity.



Several standards development organizations have already begun to develop parameters for IMT-2020 systems that go towards these IMT goals, such as the 5G Infrastructure PPP in Europe (5G PPP), who published a vision document in 2015. In this report, 5G PPP included the following as some of the targets,

⁴ SNS Telecom, *5G Wireless Ecosystem: Technologies, Applications, Verticals, Strategies & Forecasts*, February 2016, <http://www.snstelecom.com/5g>.

⁵ Recommendation ITU-R, M.2083-0 (09/2015);, *IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*, <https://www.itu.int/rec/R-REC-M.2083-0-201509-I/en>

noting that they were under discussion within the ITU, 3GPP and Next Generation Mobile Networks Alliance:⁶

- 1 000× in mobile data volume per area reaching a target of 0.75 Tb/s for a stadium;
- 1 000× in number of connected devices, reaching a density $\geq 1\text{M terminals/km}^2$;
- 100× in data rate reaching a peak rate $\geq 1\text{ Gb/s}$ for cloud applications inside offices;
- 1/10× in energy consumption over 2010, with traffic increasing dramatically;
- 1/5× end-to-end latency, reaching delays $\leq 5\text{ ms}$;
- 1/5× network management operational expenditure;
- 1/1 000× service deployment time reaching a complete deployment in $\leq 90\text{ minutes}$;
- guaranteed user data rate $\geq 50\text{ Mb/s}$;
- capable of supporting IoT terminals $\geq 1\text{ trillion}$;
- service reliability $\geq 99.999\%$ for specific mission-critical services;
- mobility support at speed $\geq 500\text{ km/h}$ for ground transportation; and
- accuracy of outdoor terminal location $\leq 1\text{ m}$.

Regulatory Challenges: Finding the spectrum for /IMT-2020

Given IMT-2020's potential importance in bringing ubiquitous connectivity, and the long timelines needed for development and deployment, discussions are already well underway regarding its regulatory needs. One of the most challenging questions remains what spectrum resources it may rely upon.

Because of the diverse technical performance criteria required to meet targets, studies of IMT-2020 technical requirements, including Report ITU-R M.2290-0, "Future spectrum requirements estimate for terrestrial IMT," published in 2013, have concluded that a diverse number of spectrum bands may be required.⁷ In Resolution 238⁸, WRC-15 resolved to undertake the appropriate studies to determine the spectrum needs for the terrestrial component of IMT in the frequency bands above 24.25 GHz to support /IMT-2020 in advance of WRC-19. These studies are currently ongoing.

These and other discussions encompass a large number of disparate criteria, all of which may or may not be satisfied by eventual systems. What is likely at this point is that to meet high expectations, IMT-2020 systems will require a combination of different approaches, different technologies, and various frequencies for different purposes. Some of these are existing technologies, such as greater deployment of small cell or employment of satellite links, and others are newer technologies that are seen as revolutionary, such as the use of millimeter-wave frequencies for wireless backhaul and/or access.

IMT-2020 systems will take advantage of many of the advances in network architectures and software, such as software-defined networking (SDN), network function virtualization (NFV), network slicing, advanced

⁶ 5G PPP, *5G Vision: The 5G Infrastructure Public Private Partnership: the next generation of communication networks and services*, February 2015, <https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf>

⁷ Report ITU-R M.2290-0 (12/2013): *Future spectrum requirements estimate for terrestrial IMT* (<http://www.itu.int/pub/R-REP-M.2290-2014>)

⁸ RESOLUTION 238 (WRC-15): Studies on frequency-related matters for International Mobile Telecommunications identification including possible additional allocations to the mobile services on a primary basis in portion(s) of the frequency range between 24.25 and 86 GHz for the future development of International Mobile Telecommunications for 2020 and beyond; Final Acts WRC-15, page 296 (<http://www.itu.int/pub/R-ACT-WRC.12-2015/en>)

modulation access schemes, and cloud computing systems. These tools allow for greater virtualization and centralization of operations, which can reduce cost and increase flexibility in meeting customer and network requirements. It is expected that IMT-2020 will also use multiple frequency bands. Some of bands below 6 GHz are already available and globally harmonized for IMT. A number of other bands between 24.25 GHz and 86 GHz are under active study at the ITU-R. What spectrum resources IMT-2020 systems will use in the 5G future will depend on the direction of these discussions.

3.1.2 Small Cells

To meet the demand for wireless broadband, future generations of wireless technology and services must continue to increase their yield of bits per hertz per second. Future wireless traffic demands may also require new wireless network architectures as well as new approaches to spectrum management. For example, small cells using IMT technologies have the ability to enhance capacity and per-user throughput, as well as reducing costs and uniquely offering tight cooperation with the macro coverage layer.

Small cells using low power nodes are considered promising to cope with the expected mobile traffic demands, especially for hotspot deployments in indoor and outdoor scenarios. They are often employed by mobile network operators to extend the reach and quality of their networks. Small cells, which can include femtocells, picocells and microcells, provide a small radio footprint ranging from 10 meters within urban areas to 2 km in rural locations. Mobile operators often use small cells to extend their service coverage or to increase network capacity in areas of high demand. They may have an important role to play in enabling IMT-2020, which many expect to rely on heterogeneous networks (discussed below) of different cell sizes to provide more ubiquitous connectivity. Providing backhaul to these small cells can be challenging since they are often in hard to reach places and require carrier grade connectivity.

3.1.3 Millimeter Waves

One of the design elements under consideration to enable IMT-2020 to meet high demand is to use millimeter-wave frequencies (between 30 and 300 GHz) to deliver faster, higher-quality services. Since at these frequencies, allocations to the mobile service have a larger bandwidth and the transmission range of millimeter waves is relatively shorter than in lower frequency bands – in the hundreds rather than thousands of meters – mobile network operators may find millimeter waves useful to support the use of small cells in their networks.

The recent World Radiocommunication Conference 2015 (WRC-15)⁹ debated bands to study for IMT for 2020 and beyond. It decided to consider the following bands, many of which are millimeter-wave bands: 24.25-27.5 GHz, 31.8-33.4 GHz, 37-40.5 GHz, 40.5-42.5 GHz, 42.5-43.5 GHz, 45.5-47 GHz, 47-47.2 GHz, 47.2-50.2 GHz, 50.4-52.6 GHz, 66-76 GHz and 81-86 GHz. Since several other services use portions of these bands (e.g. fixed, radiolocation, radionavigation and different satellite services) and considering that parts of those bands do not have a global mobile allocation, the ITU-R will undertake compatibility studies to determine the feasibility of using these bands for /IMT,IMT-2020 (5G), for consideration and adoption by WRC-19.

ITU and IMT standards towards 5G

Both ITU-R and ITU-T have begun to specify standards and target performance criteria for IMT-2020. ITU-R Study Group 5, in particular Working Party 5D which is the leading group of IMT-2020, systems comprising the IMT-2000, IMT-Advanced and IMT-2020, is continuously driving the studies and the standardization process in full collaboration with national and regional standards development organizations, equipment manufacturers, network operators, as well as academia and industry forums.

⁹ <http://www.itu.int/en/ITU-R/conferences/wrc/2015/Pages/default.aspx>

ITU-R Working Party 5D has already produced a number of Recommendations and Reports dealing with IMT-2020 and is working following a detailed time schedule to produce a IMT standard for 5G in 2020.

ITU-T Study Group 13 established a Focus Group in May 2015¹⁰ to encourage the participation of members of other standards organizations, including experts who may not be members of ITU. The Focus Group will conclude its work at the end of 2016 and report to Study Group 13 at the beginning of the next study period. One of the primary activities of the Focus Group was to undertake a gap analysis of the standardization activities underway, based on the studies on several key technical topics and related non-radio parts of IMT-2020. The Focus Group provided a final report that addresses five study areas: high-level network architecture, an end-to-end quality of service (QoS) framework, emerging network technologies, mobile front haul and back haul, and network softwarization.¹¹

3.2 Satellite Communications Technologies

In addition to its important role in television broadcasting and video distribution worldwide, fixed and mobile satellite communications also are widely used in remote and rural areas, during times of disaster when terrestrial networks are damaged, and in support of maritime, aviation, and other vertical markets. Satellite communications form part of the Internet connectivity ecosystem, and are used to support commercial and consumer data services, such as through VSATs, residential and commercial broadband services, and M2M/IoT connections. Satellite communications are used particularly in remote and rural areas and to complement terrestrial networks by increasing resiliency, ubiquity, and capacity.

Much like others in the ICT sector, satellite network operators and manufacturers are facing a world that is hungry for more data, more speed, lower latency, and competitive pricing – all while feeling pressures on limited spectrum resources. The satellite sector is also seeing new operator and manufacturing entrants, and competitive pressures from other access technologies such as high-altitude drones or balloons aiming to provide Internet services to remote and rural areas. Can satellites remain relevant in the 5G environment?

New “breeds” of satellite technologies already are responding to these challenges. Well-established manufacturers are seeking ways to innovate traditional satellite designs, and entrepreneurs and new entrants are completely rethinking the manufacture, launch, and deployment of satellites to connect the unconnected. Advances have affected the cost, capacity, and capabilities of larger geostationary satellites and innovations in smaller satellites allow for deployment more quickly and cheaply. This section will describe three particular innovations in the satellite sector, with consideration of whether or how regulators may need to address them: high-throughput satellites (HTS), non-geostationary fixed-satellite service (NGSO FSS) satellites, and nanosatellites.

3.2.1 Geostationary High-throughput Satellites

The introduction of a new class of geostationary high-throughput satellites (GSO HTS) – high-powered, spectrally efficient satellites with spot beams offering considerably higher bandwidth than earlier versions – promises to significantly reduce the basic cost of bandwidth. Geostationary satellites operate at an altitude of approximately 35 800 kilometers (22 300 miles) directly over the equator, thus appearing to be fixed relative to the Earth.

¹⁰ ITU-T, *Focus Group on IMT-2020*, <http://www.itu.int/en/ITU-T/focusgroups/imt-2020/Pages/default.aspx>

¹¹ ITU-T, *FG IMT-2020: Report on Standards Gap Analysis*, December 2015, <http://www.itu.int/en/ITU-T/focusgroups/imt-2020/Documents/T13-SG13-151130-TD-PLN-0208!!MSW-E.docx>

There are several distinguishing features of HTS satellites compared to earlier GSO networks – primarily higher speed, greater capacity, lower cost, and increased flexibility. Older generations of GEO satellites have been limited by power, capacity, and transmission delays. HTS satellites address these challenges through the application of enhanced solar power systems, on-board processing to maximize the efficient use of every available hertz and hybrid terrestrial/satellite innovations to divert latency-sensitive traffic over shorter terrestrial routes. By 2020-2025, there will be over 100 HTS systems in orbit delivering terabytes of connectivity across the world using Ku and Ka bands, reducing unit bandwidth costs by an estimated factor of 10.¹²

Some of the new features include adjustable spot beams, which enable greater flexibility for the operator to direct capacity to suit changing demands of customers. Considering that the average lifespan of a satellite is 15 to 20 years – a period of time during which market requirements can change significantly – having the ability to make changes in footprint or offerings enables operators to remain responsive to a changing environment. These satellites are already starting to be introduced into the marketplace, with more than fifteen HTS systems in orbit now, many of which are operated by the incumbent global and regional satellite operators.¹²

For regulators, it is important to take account of the ongoing and planned investments in satellite innovations – it may cost more than \$200 millions¹³ and seven years to plan, design, and launch a new geostationary satellite. Relative to previous iterations of satellite technologies, HTS promise a more competitive market and a key enabler to meet universal broadband targets than previous iterations of satellite technologies. Careful consideration should be given to satellite spectrum resources, whether existing resources should be protected or whether or how certain spectrum resources may be shared with other services. Regulators may also take account of satellite licensing regimes, particularly for the Ka band, to allow for deployment of services when these satellites are launched in increased numbers.

3.2.2 NGSO Systems

Non-geostationary satellites (NGSOs) operate at lower orbital altitudes than GSOs – typically low-Earth orbits (LEO, around 500 to 2,000 km above the Earth) and medium-Earth orbits (MEO, between LEO and GEO: some 2,000 to 36,000 km above the Earth) or and require multiple satellites to allow for continuous commercial coverage. NGSOs have been a feature of the space science and Earth exploration domains for decades; however, new classes of commercial NGSO systems are under development, with plans to launch hundreds or possibly thousands of satellites. Promising to bring broadband anywhere in the world and to obviate the need for expensive fiber infrastructure in difficult-to-reach places, new NGSO systems have received a new wave of investment from key players, both from within and outside the traditional satellite industry. They are being designed with the intention of connecting users in under-served areas.

¹² European Satellite Operators Association (ESOA);

¹³ The Economist, “Nanosats are go!,” 7 June 2014, <http://www.economist.com/news/technology-quarterly/21603240-small-satellites-taking-advantage-smartphones-and-other-consumer-technologies>

Regulatory Challenges: Mega NGSO Constellations

The ITU Radio Regulations provide the regulatory framework for filing, notification, and coordination of satellite networks, including for NGSO networks. Effective coordination between different users is critical to ensure that spectrum is used efficiently and to prevent harmful interference. Operators of planned NGSO networks have submitted to the ITU the required satellite filings, through notifying administrations and, in some cases, are already in the process of coordinating their networks with other affected administrations and operators using the regulatory framework established by the ITU in the 1992-2003 timeframe to enable the first generations of NGSO constellations to coexist with GSO and terrestrial networks. Is this framework fully adequate for these planned “mega-constellations”?

WRC Resolution 86 (Rev. WRC-12) provides a framework for ongoing studies of the satellite regulatory framework including satellite filing, notification, and coordination procedures. While WRC-15 did not make any changes to address NGSOs, the ITU-R is able to study this topic in the lead up to WRC-19, reviewing the current rules and evaluating whether any changes are needed to ensure the most efficient use of the orbital resource.¹⁴

These constellations aim to provide direct broadband capacity to users all around the globe, extending terrestrial broadband connectivity and providing direct-to-consumer Internet connectivity in remote areas. Given their relatively low altitude (compared to GSO satellites), these networks will have low latency (often competitive with terrestrial fiber), high capacity, and wide coverage of the globe. The links they can provide could support mobile backhaul, traditional fixed services, or offer broadband capacity directly to end-users.

3.2.3 Nanosatellites

Some of the most exciting advances in satellite technology have occurred in the “small satellite” realm. Known as nanosatellites or picosatellites, these small and lightweight satellites are lowering the costs of entry and expanding the range of applications possible. In the next five years or so some 1 000 small satellites are expected to be launched into lower Earth orbits, fueled by the rapid development of low-cost commercial launch vehicles.

Nanosatellites have proved popular with research institutions, government agencies, and industry alike. Because of their low cost, they are enabling the field of satellite players to expand very quickly and bring to market a wide variety of innovative applications – from Earth exploration, to data imaging, tracking, and weather sensing. Communications networks are being developed using large number of such satellites to provide useful capacity.

Compared to their larger cousins, nanosatellites bring a number of benefits, including:

- **Innovative designs** – Nanosatellites take advantage of recent advances in consumer electronics. Small-satellite engineers are able to incorporate the latest technologies into the design, particularly many of the sophisticated functions from smartphones.
- **Standardized designs** – Some, known as cubesats, follow a standard design. Cubesats are 10 cm (4 inch) long each side, weighing 1.3 kg (2.9 lb) or less. This makes them easier to mass-manufacture, simpler to launch into space, including as a secondary payload, and able to be easily combined into larger versions two, three, or more units in length for specific purposes.

¹⁴ See Agenda and presentations from: ITU Workshop on the Non-GSO Satellite Issues; Geneva, 21st April 2016; <http://www.itu.int/en/ITU-R/space/workshops/2016-NGSO/Pages/programme2.aspx>

- **Lightweight** – These satellites are a fraction of the size and weight of the larger satellites, making them easier to manufacture and launch. They often “piggy-back” on other launches, or in some cases have been deployed from the International Space Station.
- **Low cost** – According to an estimate in the *Economist*, the cost of a nanosat of CubeSat dimensions might cost \$150 000 - \$1 million (including the launch), compared to a full-sized satellite system cost exceeding \$ 200 million.¹⁵
- **Shorter life** – Missions are typically just one to two years in LEO, before re-entering the atmosphere and burning up. Some operators intend on replacing their fleet often, such as Planet Labs, which plans on replacing some of its satellites with newer versions every year.

WRC-15 considered whether existing satellite regulatory frameworks were sufficient to accommodate nanosatellites and it was determined that no changes were required. Additionally, the Radiocommunication Assembly 2015 adopted ITU-R Resolution 68 entitled “*Improving the dissemination of knowledge concerning the applicable regulatory procedures for small satellites, including nanosatellites and picosatellites*”¹⁶, which aims to ensure regulators and small satellite operators are informed about the proper ITU regulations and filing procedures, including through training and capacity building. Regulators should consider providing clarification and information for national small satellite developers to guide them on how they may apply for licenses through domestic rules, including any applicable ITU Radio Regulations filing requirements. Having clear information on any regulatory requirements will help stimulate growth in this sector, and ensure an interference free environment. Additional experiences of nanosatellite operators will also help inform any future studies of the ITU-R.

WRC-15 also invited WRC-19 to study the spectrum requirements for telemetry, tracking, and command in the space operation service for the growing number of non-GSO satellites with short duration missions.

¹⁵ The Economist, “Nanosats are go!,” 7 June 2014, <http://www.economist.com/news/technology-quarterly/21603240-small-satellites-taking-advantage-smartphones-and-other-consumer-technologies>

¹⁶Resolution ITU-R 659 (WRC-15) ‘*Studies to accommodate requirements in the space operation service for non-geostationary satellites with short duration missions*’; Book of ITU-R Resolutions, Edition 2015, issued from last Radiocommunication Assembly, RA-15 (10/ 2015): <http://www.itu.int/pub/R-VADM-RES/en>

Regulatory Challenges: Nanosatellites and space law

By lowering barriers to entering space, nanosatellites have brought many new actors who may not be familiar with national and international regulatory frameworks. Consequently, many small satellite operators do not register their satellites according to the agreed national and international procedures for registration and de-orbiting. Lack of compliance makes it more difficult to get a true sense of the number of satellites launched as well as to then track those small space objects in orbit. Such missions do not always fully comply with international obligations, regulations, and relevant voluntary guidelines, including those related to orbital debris. This can increase the risk to other fully compliant space missions and may threaten the long-term sustainability of low earth orbit space activities.

In 2015, the ITU Symposium on Small Satellite Regulation and Communication Systems met to discuss some of these issues, especially interference and registration issues. The outcome was the Prague Declaration, in which regulators acknowledged the challenges small satellites can pose, urged conformity to existing international instruments, and resolved to increase awareness of existing regulatory and licensing requirements for small satellites¹⁷. The ITU Radiocommunication Assembly (RA-15) also recognized this (See Resolution ITU-R 68).

3.3 High-altitude Platform Stations (HAPS)

While previously providers of communications services have fallen clearly into one of two categories – satellite or terrestrial – new efforts are underway to give a second wind to a delivery platform, which is physically located between the two: high-altitude platform stations (HAPS), placed on air above 20 km height.¹⁸

Regulatory Challenges: Finding a place for HAPS in telecommunications regulations

As part of its agenda, WRC-19 will consider additional spectrum requirements for gateway and fixed terminal links for HAPS. Spectrum identifications and international regulations already exist for HAPS, but these may not be sufficient for the delivery of broadband services. Studies are underway in ITU-R Study Group 5 in preparation for WRC-19¹⁹. It is expected that national regulatory frameworks would need to be adopted for this type of technology. These needs may include a licensing framework to authorize operators to operate unmanned airplanes or balloons as well as provide communications capacity.

While the ITU-R has studied the delivery of radiocommunication services over HAPS for years, operational HAPS systems communications services have yet to be realized. Recent improvements in lightweight aircraft technology offers potential for realizable HAPS systems. The growing urgency to expand the availability of broadband has renewed the interest in these platforms.

Improvements in composite materials, low-power computing, battery technology, and solar panels paved the way for this concept. These planes will be kept approximately 20 km above the Earth's surface, enabling them to provide broadband services to a wide area below,

¹⁷ See “*Prague Declaration on Small Satellite Regulation and Communication Systems*”, issued from: ITU Symposium and Workshop on small satellite regulation and communication systems, Prague, Czech Republic, March 2015; <http://www.itu.int/en/ITU-R/space/workshops/2015-prague-small-sat/Pages/default.aspx>

¹⁸ According to national and international spectrum regulations, both HAPS and Stations placed on land masses are part of terrestrial stations, in opposition to space stations, i.e., satellites

¹⁹ Resolution 160 (WRC-15): *Facilitating access to broadband applications delivered by high-altitude platform stations*; Final Acts WRC-15, page 261 (<http://www.itu.int/pub/R-ACT-WRC.12-2015/en>)

allegedly with latency similar to terrestrial technologies. These planes will use free-space laser communications or radio frequencies to connect to other planes and the ground. Powered by solar panels, they are planned to remain in the air for months at a time. Flexibility and ease of deployment are its biggest advantages, noting their ability to move easily to new locations. This flexibility enables them to be relocated in order to meet demand and the changing requirement of the operator or service provider's business plan

With respect to spectrum resources for these applications, the ITU Radio Regulations currently contain several frequency bands designated for HAPS in 2 GHz, 6.5 GHz, 27/31 GHz and 47/48 GHz ranges. However, these bands have geographical limitations and may not be large enough to provide high-rate broadband. The ITU-R is currently studying potential additional bands for HAPS in the bands 21.4 – 22 GHz, 24.25-27.5 GHz and 38-39.5 GHz allocated to the fixed service. WRC-19 will consider the results of these studies and could take decision on designation of some additional bands for HAPS.

Engineers are also studying the upper parts of spectrum, including optical bands. Recent test deployments of stations delivering broadband from approximately 20 km above ground have demonstrated the potential of providing connectivity to underserved communities with minimal ground-level infrastructure and maintenance. Although results of recent tests still need some verification, HAPS can probably be an effective tool to help close the digital divide in remote communities, particularly those with challenging terrain or climate. These stations are also highly resilient in the face of natural disasters and therefore can be an effective tool for disaster recovery. Some other potential applications of broadband delivered from HAPS include public protection and disaster relief, distance learning, tele-medicine and healthcare.

3.4 Evolving platform stations

Leveraging on new and emerging technologies, platform stations are evolving. Facebook is currently developing a system known as project Aquila. It has designed a plane approximately the weight of an automobile, which is able to stay at an altitude of 60 000 feet for months at a time.²⁰ This space plane will use lasers to transmit data between planes and to terrestrial stations within 50 kilometers, which can then provide Wi-Fi or 4G coverage locally.²¹

Separately, Google is developing the capability to use drones to provide wireless internet access using millimeter wave transmissions, which could offer up to 40 times more than today's 4G LTE systems. Google plans for thousands of high altitude drones to deliver Internet access around the world.²²

Google is also developing a more traditional HAPS project, known as Project Loon, which will rely on balloons to deliver connectivity to those on the ground. This project, which has officially been in development since 2013, aims to provide 4G LTE internet via balloons traveling through Earth's stratosphere. The system has been tested in New Zealand, California, and Brazil. Google hopes Loon can eventually provide high-speed Internet to those in rural and underserved areas.²³

²⁰ Danny Yadron and Jemima Kiss, "Facebook F8: Zuckerberg shows off chat bots, VR... and a dig at Donald Trump," *The Guardian*, 13 April 2016, <https://www.theguardian.com/technology/2016/apr/12/mark-zuckerberg-facebook-donald-trump-f8>

²¹ Ania Nussbaum and Robert Wall, "Aquila, Facebook's First Drone for Internet.org," *Wall Street Journal*, 31 July 2015, <http://blogs.wsj.com/digits/2015/07/31/the-aquila-facebooks-first-drone-for-internet-org/>

²² Mark Harris, "Project Skybender: Google's secretive 5G Internet drone tests released," *The Guardian*, 29 January 2016, <https://www.theguardian.com/technology/2016/jan/29/project-skybender-google-drone-tests-internet-spaceport-virgin-galactic>

²³ Ben Thompson, "What is Google's Project Skybender?" *Christian Science Monitor*, 31 January 2016, <http://www.csmonitor.com/Technology/2016/0131/What-is-Google-s-Project-SkyBender>

4 Changing Architectures and Complementary Technologies

The ICT industry is actively developing new ways of building networks to accommodate increased demands for data – some that centralize resources in order to attain economies of scale, others that distribute resources to the edges of networks so as to respond more flexibly to changing needs. These innovations are also emerging in part because of the increasing role that software is assuming relative to hardware in network technologies. This includes software defined networking (SDN), the practice – rapidly growing over the past five years – of transforming control of high-level network functions into software abstractions. SDN, which allows for greater agility, flexibility, and control in large networks, forms the foundation of many emerging network technologies. Some of these technologies, such as cloud computing, are already widespread and well understood, while others may be less known.

Regulators need to be aware of these developments and evaluate how existing regulatory frameworks may already be able to accommodate them. They may also need to consider where regulatory reforms are necessary to address new challenges, for example security, and allow these innovations to take shape. Importantly, the following section demonstrates the rapid pace of research and development being undertaken to meet current and anticipated challenges in the ICT sector. Governments can also play a role in supporting and stimulating research and development, and in providing an economic and legal environment supportive of innovation and entrepreneurship.

4.1 Advances in Network Architectures

4.1.1 Cloud Computing

Already a well-recognized technology, cloud computing is a major disruption to the ICT industry and is still evolving as more and more consumers and businesses move into the cloud. It is enabling new cellular network architectures such as cloud-RAN, discussed below, and will become increasingly important to the delivery of big data services and the IoT.

Cloud computing is an on-demand computing method that enables users to access shared computing resources and data over the Internet. Working on a principle of centralization, this model enables pooling of configurable computing resources (for example network servers or storage) as well as applications and services. This centralization provides economies of scale, which cloud service providers can leverage to deliver cheaper computing solutions to multiple users. Some of the major advantages cloud computing provides to users and enterprises are:

1. **Affordability** – Users and enterprises, especially small and medium sized entities, are able to access computing resources without upfront infrastructure costs.
2. **Scalability** – Enterprises can sign up to different packages depending on their business need, with the possibility to upgrade and downgrade as needed.
3. **Efficiency** – Enterprises can focus on their core business instead of spending resources on IT problems.
4. **Availability** – Users are able to access services over the Internet regardless of their location and the type of devices used, encouraging better collaboration through “anywhere, anytime” access to IT for users located around the world.
5. **Cost Savings** – Greater automation of processes can lead to reduced labor costs and a reduction in human errors.

Regulatory Challenges: Weighing the benefits and challenges of cloud computing

Cloud-based technologies are central to many of the technologies and architectures discussed in this report. ITU-D Study Group 1 is currently examining cloud computing in Question 3/1, “Access to cloud computing: challenges and opportunities for developing countries.”²⁴ The question notes that cloud computing can be “a possible solution to the lack of adequate computing resources” in developing countries, and provides benefits both in the form of economies of scale and flexibility of use. The responsible Rapporteur Group is expected to produce a final report in 2017 containing analysis of factors influencing effective access, capacity building guidelines, and draft guidelines or recommendations.

Despite the potential benefits cloud solutions can bring, they can raise regulatory questions regarding privacy, security, and international transfers of data. Centralized systems, such as cloud networks, may offer greater protection from threats by simplifying and centralizing control, and cloud providers likely are able to provide more up to date and state-of-the-art security protections than a small business could afford; however, such systems also raise the stakes that security failures may impact a wider population. Regulators should examine existing national cybersecurity frameworks to ensure consistency with international best practice. Cloud systems are also generally sensitive to international restrictions on the transfer of data. By centralization resources to attain economies of scale, data sometimes needs to flow across borders to where it can be most efficiently processed. Regulations that provide for international transfers of data are therefore important to gaining access to many cloud services.

4.1.2 Cloud-RAN Using Fronthaul

A cloud radio access network (Cloud-RAN or C-RAN) was first promoted by China Mobile Research Institute in April 2010, nowadays several other operators are considering this technology very promising for the development of future mobile networks. C-RAN is a centralized cloud-based architecture for radio access networks that supports a wide variety of networks including 2G, 3G, 4G and future wireless standards. It is based on two major ideas to improve base station baseband processing: centralization and virtualization.

Centralization is key to improving performance and reducing operational costs (such as support and maintenance costs). This is enabled by a practice known as “fronthaul”, where the baseband unit (BBU, which processes user and control data) and the radio unit (RU, which generates radio signals transmitted over antennas) are located further away from each other than in the traditional backhaul model. In this model, the BBU is separated from the RU and relocated to a centralized and protected location – up to several kilometers away – where it can serve several remote radio heads (RRHs) also known as remote radio units (RRUs). The optical links that connect the centralized BBU to the multiple RRHs are referred to as fronthaul.

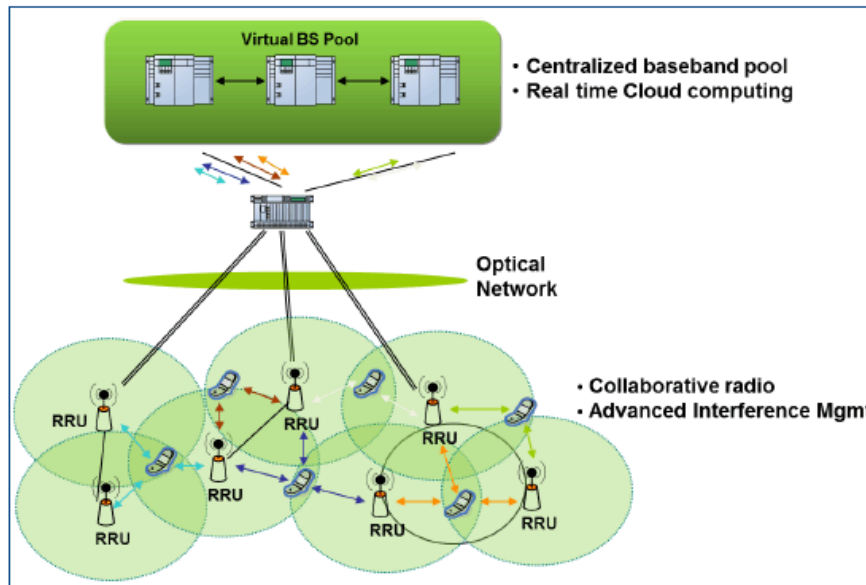
This stands in contrast to the conventional backhaul model, in which the BBU resides close to the RU within a typical macro cell, connected to the larger network infrastructure through long distance optical links. This allows for tighter coordination between cells than is available in traditional networks dependent on backhaul. This is a critical feature especially in HetNets and when small cells are deployed in the same frequency bands as the macro cells (especially in LTE), as a way to more effectively manage interference between cells and increase user data throughput.

Virtualization rooted in cloud computing aims to reduce capital expenditures by applying network function virtualization (NFV) to RANs. This allows operators to use commercial servers for base station hardware instead of custom-built products. This has a number of advantages: it allows operators to leverage economies of scale; by decreasing the complexity of hardware needs, it decreases the time to develop and

²⁴ ITU-D, *Question 3/1 Access to cloud computing: challenges and opportunities for developing countries*, <http://www.itu.int/net4/ITU-D/CDS/sg/rgqlist.asp?lg=1&sp=2014&rgq=D14-SG01-RGQ03.1&stg=1>

deploy new services; and it enables dynamic shared resource allocation and supports multi-vendor, multi-technology environments.

There are reports that deployments of C-RAN systems have already begun. This technology has attracted various equipment vendors working in collaboration in the recent few years. Research and development on C-RAN is also on-going, and it is expected to gain popularity in the near future.



Cloud-RAN is a cellular architecture that separates the “remote” radio head (RRH) from centralized baseband unit pool through long distance fronthaul optical links.²⁵

4.1.3 Mobile Edge Networking (MEN)

Mobile edge networking (MEN) or mobile edge computing (MEC) applies the principle of decentralization of resources to better meet the needs of mobile network operators and users. MEN is a network architecture that enables application developers and content providers to deploy cloud computing capabilities (for example a cloud server) and IT services nearer to the edge of the mobile network – performing a task that could not be achieved with traditional network infrastructure.

The idea of running applications and the related processing task closer to the cellular customer enables an improved quality of experience to users, lower latency, higher bandwidth, as well as real-time access to radio network information. Mobile core networks are also relieved from further congestion and can efficiently control resources for a more optimized network. This helps operators cope with increasing demand for ubiquitous, high speed, and high performance Internet access.

ETSI and MEC standards

New MEC industry standards and deployment of MEC platforms will help generate new revenue for operators, vendors, and third-party service providers. Currently, the European Telecommunications Standards Institute (ETSI) Industry Specification Group (ISG) is conducting work on MEC. The work of ETSI MEC aims to define elements needed in a specification, and to address the necessary legal and regulatory requirements for wider deployment.

MEN infrastructure consists of standardized hardware resources and a software-implemented virtualization layer. High-volume, off-the-shelf IT hardware is used to achieve economies of scale and enables rapid and cost-effective upgrades. This creates a new ecosystem and value chain, allowing operators to open their RAN’s edge to authorized third parties, encouraging rapid deployment of innovative applications and

²⁵ Global Information Inc., “C-RAN and LTE-Advanced: The Road to “True 4G”, 4G’ & Beyond,” 28 October 2013, <https://www.gii.co.jp/report/heav288660-c-ran-lte-advanced-road-true-4g-beyond.html>

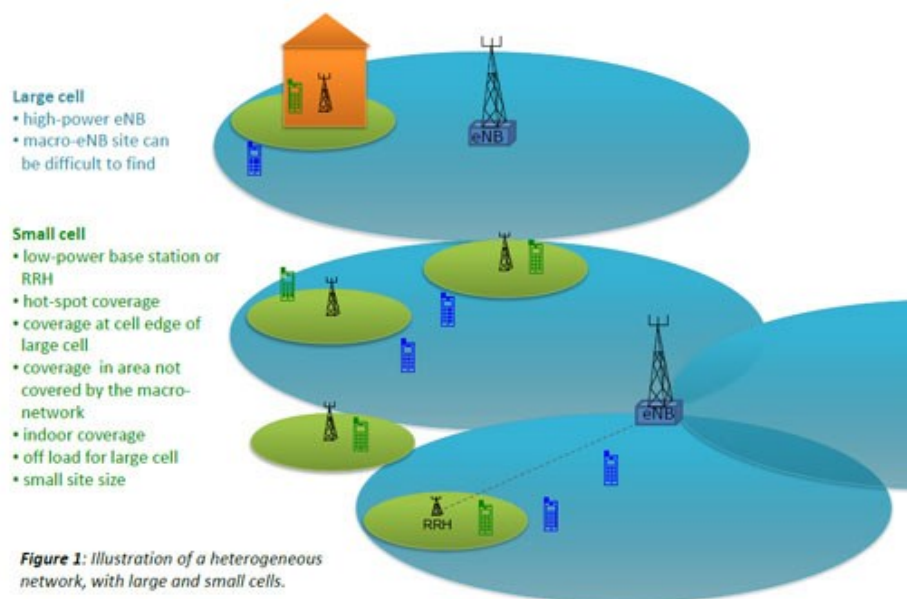
services to the mobile subscribers. It allows software applications to tap into local content and real-time information about local access network conditions.

4.1.4 **Heterogeneous Networks (HetNets)**

In addition to changing the way that they carry out computing and route network functions, network operators are finding that they can improve performance by refining the architecture of the wireless portion of their networks. Accordingly, heterogeneous networks (HetNets) are gaining popularity as a mechanism of expanding network coverage through the deployment of different sized cells and types of technology.

A typical HetNet comprises multiple radio access technologies, architectures, transmission solutions, and base stations of varying transmission power. This technique represents an evolution of existing network technologies, rather than a new type of network technology itself.

Combining a variety of technologies together allows the most appropriate option to be chosen for a given area and helps provide ubiquitous service. Operation of the network in different cell sizes can also be used to satisfy different coverage needs and augment overall network capacity. For example, small cells such as femtocells and Wi-Fi hotspots can be deployed within buildings, whereas traditional macro cells are needed to provide general coverage for mobile users. Cell selection techniques can optimize these choices. Figure 1 illustrates the potential configuration of a HetNet, using both indoor and outdoor small cells.²⁶



If all these parts can provide a high level of performance, they can appear to the user as a single seamless network. This is also useful for mobile operators who are looking to adopt cellular HetNets to meet coverage and capacity goals when demands on the mobile networks rise - for example at stadiums or events with large numbers of people. The operators can offload data away from the central backhaul network through other technologies in the HetNet, allowing better use of the radio spectrum and an improved user quality of service.

4.1.5 **Network Slicing**

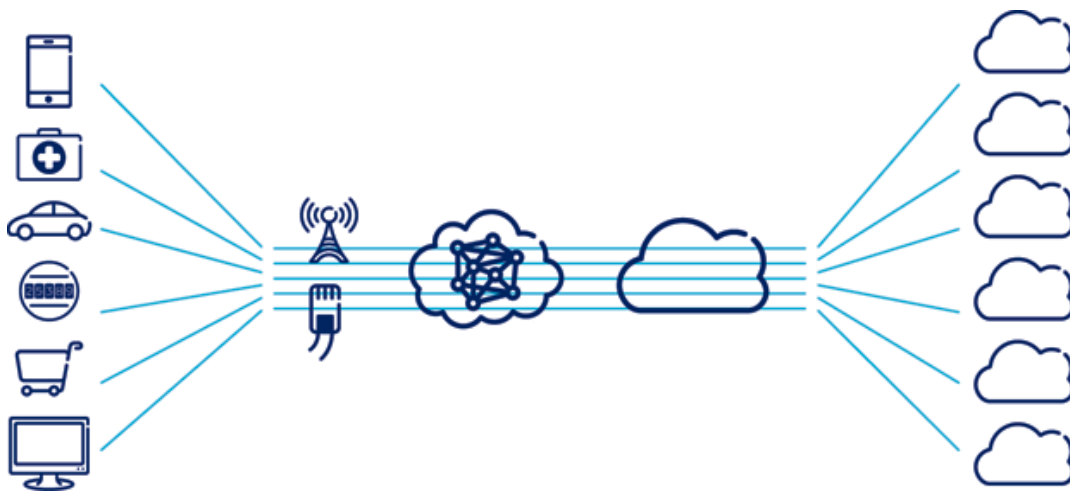
Network function virtualization techniques discussed above enable mobile operators to deploy a number of new features. One of the most discussed is network slicing, a mechanism proposed for 5G/IMT-2020

²⁶ Jeanette Wannstrom and Keith Mallinson, *HetNet/Small Cells*, <http://www.3gpp.org/hetnet>

systems that operators can use to support multiple virtual networks behind a single air interface. The technique “slices” the network into multiple virtual networks to support different RANs of different service types across the fixed part of the network, both in the backhaul and the core networks.

Traditionally, operators build network systems with certain predictable network traffic and expected growth. This type of vertical architecture is difficult to scale or to adapt to changing demands, making it harder to quickly meet the requirements of emerging use-cases. Network Function Virtualization (NFV) and software-defined networking (SDN) provide the tools to create networks with a greater degree of abstraction by enabling vertical systems to be broken apart into building blocks, resulting in a horizontal network architecture which can be chained together to focus on providing certain kinds of service.

Network slicing allows an operator to deliver diverse services over one RAN infrastructure, rather than constructing different RAN infrastructures for discrete services.²⁷



This enables creation and expansion of separate logical nodes and functions for a specified group. In IMT-2020 systems, the transformation of a network into slices allows connectivity to be defined by a number of software functions that provide a certain coverage area, duration, capacity, speed, latency, robustness, and security parameters as needed. Network slicing enables IMT-2020 to be defined according to the requirements of users and operators, and to provide networks-on-demand supporting a wide range of use cases ranging from low-cost, low power, and low speed Internet of Things (IoT) connections to more bandwidth hungry video streaming connection.

Network slicing enables networks to be defined with greater flexibility and therefore provides a wide range of connectivity services. Rather than build multiple networks to support many different types of services, operators using network slicing can build a single, virtually segmented network to support many different types of users and applications with different needs. Since each slice is customized to match the complexity required for that service, network slicing can also enable more accurate billing according to usage by improving insights on network utilization.

²⁷ Ericsson, *White Paper: 5G systems – enabling industry and society transformation*, 26 January 2015, <http://www.ericsson.com/news/150126-5g-systems-enabling-industry-and-society-transformation> 244069647_c

Network slicing is rapidly gaining acceptance and is widely expected to be integral to IMT-2020 future mobile system designs to support the highly differentiated characteristics of various connections envisioned in a IMT-2020 system. The Republic of Korea's SK Telecom recently announced a partnership with Ericsson, an early leader in developing network slicing, to develop network slicing for use in a IMT-2020 network.²⁸ This continues their existing partnership in building a 5G testbed.

4.2 Advances in Software

Many have observed that advances in hardware processing power have begun to slow.²⁹ As processors have become smaller and smaller, designers have begun to reach the limits of miniaturization. This does not necessarily mean that advances in computing will stop, but that future advances may come in the form of software innovations, rather than hardware. Correspondingly, "softwarization" has become a broad trend, referring to the ever more important role that software has come to play today in the drive to develop more efficient, cost-effective, and agile delivery of ICT services. More advanced software is coming to replace more advanced or specialized hardware, and is increasingly used to provide improved performance and greater efficiencies in the ICT and telecom industries.

Regulators should take account of these advancements and ensure that any applicable regulatory frameworks allow sufficient flexibility to allow for software based changes or upgrades without requiring a modification to the licensing or regulatory requirements, particularly if regulations are tied to specific equipment. Support should be given to research, development, and standardization efforts in developing these software-based techniques to enhance networks.

4.2.1 Network Function Virtualization (NFV)

Network operators are looking for ways to handle new types of demand and develop services more quickly. NFV seeks to meet this challenge by using IT virtualization techniques to transform conventional network node functions into software building blocks that can be mixed and matched to provide network functionalities rapidly.

Rather than use customized hardware for each network function as in conventional network nodes, NFV allows operators to substitute software to simulate specialized hardware, which can run on generic, standardized equipment such as high volume servers, switches, and storage. Network service providers are increasingly finding that this capability improves the flexibility of service provisioning and reduces the time to market of new services.

²⁸ Ericsson, *Ericsson and SK Telecom to collaborate on 5G network slicing*, 27 July 2015, <http://www.ericsson.com/news/1942903>

²⁹ Technology Quarterly, "After Moore's Law," *The Economist*, 12 March 2016, <http://www.economist.com/technology-quarterly/2016-03-12/after-moores-law>

By relying upon virtualized, as opposed to physical, infrastructure, NFV-based services provide other benefits such as high availability, ease of scalability, improved performance quality, and more effective network management. NFV is expected to support a wide range of fault tolerance options and enable service providers to employ redundant resources to meet specific high availability requirements.

NFV has proven a popular standard since its introduction and has supported various applications such as virtualization of mobile base stations, platform as a service (PaaS), and content delivery network (CDN). It also forms the foundation of other critical advance such as C-RAN and network slicing. Various NFV products have been announced or built and the ecosystem is forming at a rapid speed.

ETSI discussions of NFV

ETSI has formed an Industry Specification Group for NFV (NFV ISG),³⁰ which includes representatives of European and international telecommunications operators, to evaluate and discuss standards for the technique. It published its first white paper describing NFV in 2012,³¹ and has since produced a series of white papers, as well as reports on standard terminology, potential use cases, and relevant security and regulatory considerations.

4.2.2 Cognitive Computing

Cognitive computing employs data mining, pattern recognition and natural-language processing to mimic the processes of human brain in order to be able to learn. It addresses complex situations where ambiguity and uncertainty exist, usually in a dynamic and information-rich environment where data can also change frequently. The aim of cognitive computing is to offer better insight by synthesizing information, context, and possible influences, and to produce answers in natural language.

Cognitive systems are typically:

- **Adaptive** – They are able to learn as information changes.
- **Interactive** – Especially with users as well as with other processors and devices.
- **Iterative and stateful** – They are able to find extra input information and remember previous interactions.
- **Contextually sensitive** – They are able to understand, identify and extract contextual elements such as meaning, syntax, time, location, regulations, goals, and so on.

Cognitive computing adds an extra layer of intelligence, enabling industry to provide recommendations that are more relevant to customers, proactively and in real time. For example, in the healthcare industry, a physician could make use of more data or attributes in real time to improve the accuracy of diagnosis of a patient, rather than making use of only commonly selected attributes under the conventional method.

Cognitive computing is still a new and developing type of computing. It requires more accurate models of how the human brain senses, reasons, responds to stimuli, and draws conclusions before its full benefits can become widespread. Nevertheless, the technology has the potential to be used in many different industries, especially those that are data-rich. Cognitive computing contrasts with the traditional approach to big data, in which a company hoping to make sense of their data would use data warehouses, meaning insights could not be gained in real time.

³⁰ European Telecommunications Standards Institute, *NFV Industry Specification Group*, <https://portal.etsi.org/tb.aspx?tbid=789&SubTB=789,795,796,801,800,798,799,797,802>

³¹ ETSI NFV Industry Specification Group, *Network Functions Virtualisation An Introduction, Benefits, Enablers, Challenges & Call for Action*, 22 October 2012, https://portal.etsi.org/NFV/NFV_White_Paper.pdf

Spotlight: IBM and the Cognitive Internet of Things

IBM, which has been developing the technology over the past few years, has worked with partners to implement the technology for healthcare, financial services, and other cross-industry applications. Cognitive computing is also expected to play a key role in real time management of the vast increase in data collection and the complex systems of interconnections generated by the Internet of Things. IBM is already attempting to develop these capabilities through its Watson IoT Cloud.³² Based in Munich, the project will serve as a test bed of cognitive IoT services, targeting the automotive, electronics, manufacturing, healthcare, and insurance industries.

4.2.3 Delay-tolerant Networking (DTN)

Delay-tolerant networking (DTN) can be employed when networks lack an end-to-end path, for example due to limits of wireless radio range, scarcity of mobile nodes, energy resources, or presence of noise. It accomplishes this by using a store and forward approach, ensuring no information is lost even when a connection is interrupted. The data therefore moves incrementally through the network to reach its final destination.

Many communication environments can benefit from DTN, such as those with intermittent connectivity, long or variable delay, asymmetric data rates or high error rates such as rural areas with poor infrastructure. DTN accommodates long disruptions and delays between and within networks, and supports the mobility and limited power of evolving wireless communications devices. It can also accommodate many kinds of wireless technologies including radio frequency (RF), ultra-wide-band (UWB), and free-space optical technologies.

4.2.4 Self-organizing Networks (SON)

Self-organizing networks (SON) are seen as essential for today's complicated cellular networks that need the ability to self-configure, organize, optimize, and also "self-heal" when fault occurs. The following are some of the key features of a SON:

- Self-configuration enables simple plug-and-play of newly deployed nodes. For example, the nodes are expected to configure aspects of themselves such as the cell identity, transmission frequency, and power. This facilitates faster cell planning and roll-out.
- Self-optimization includes optimization of coverage, capacity, handover, and interference to improve capacity. To accomplish this, load level and information on available network capacity need to be maintained and exchanged between the network nodes.
- Self-healing includes features for automatic detection and removal of failures and automatic adjustment of parameters.

SON techniques are increasingly popular among operators, who can benefit from significant improvements in capital and operational expenditure. It can reduce costs by reducing the level of human intervention needed, optimizing the use of resources, and protecting the network by reducing errors. It may require larger upfront investments from the operator initially, however the returns are expected to be even larger and could be essential to long-term growth. To users, SONs can help provide lower costs and better network performance.

³² IBM, *Watson Internet of Things*, <http://www.ibm.com/internet-of-things/>

4.3 Radio and Antenna Technologies

4.3.1 MIMO

Multiple-input and multiple-output (MIMO) is an antenna technology for wireless communications in which multiple antennas are used at the source transmitter as well as the destination receiver. This method multiplies the capacity of a radio link and is also able to exploit multipath propagation.

In conventional wireless communications, a single antenna is usually used at the source and at the destination. One of the common problems this approaches faces is multipath effects, whereby obstructions such as a hill or buildings scatter signal wavefronts, causing it to travel in many different paths to reach its destination. These signals will therefore arrive at different times and wave phases, fading each other and causing errors and a reduction in data speed. The use of multiple antennas on the other hand takes advantage of this phenomenon by allowing signals to be transmitted along multiple paths, bouncing off walls, ceilings, and other obstructions to reach the antenna at different angles and at a slightly different times. By enabling the antennas to carefully synchronize and add these data streams, MIMO can increase capacity, reliability, and range. This can be done by handling the multi-path signals of spatial multiplexing MIMO using orthogonal frequency-division multiplexing (OFDM) or orthogonal frequency multiple access (OFDMA).

The use of MIMO has already been incorporated into the latest mobile communications standards such as 3GPP and 3GPP2, Long-Term Evolution (LTE) and High-Speed Packet Access Plus (HSPA+). It is expected to be integral to future IMT-2020/5G standards, especially the use of massive MIMO at the base transceiver station. This usually employs a large number of antennas, typically more than 64, and will be key to achieve the performance targets for IMT-2020/5G.

4.3.2 Beamforming

Beamforming is a signal processing technique realized by transmitters and receivers that use MIMO technology. Antennas employing beamforming focus their radiations toward the source (or destination) instead of spreading out into the atmosphere in all angles as in omnidirectional transmission and reception. This is done by a beamformer that controls the phase and relative amplitude of the signal at each antenna, creating an intended radiation pattern.

Conventional beamformers use a selective and fixed set of weightings and phasing to combine the signals in the array. The adaptive beamforming technique on the other hand is able to automatically adapt the beamforming according to different situations. Adaptive beamforming antennas, also referred to as a “smart antennas,” can support more than one user on the same frequency, as long as they are in different directions, by steering the separate antenna beams at each user, hence focusing the energy in the respective directions. This allows concurrent transmission in one area, reducing interference to other users and increasing the energy efficiency and network capacity of cellular systems dramatically.

This capability is particularly important for IMT-2020 networks, where interference needs to be carefully controlled to support high throughput for a large number of users. Newer technology such as field-programmable gate arrays (FPGAs) are able to handle high data rates in real-time using reconfigurable interconnects, using a combination of hardware and software technology, making it particularly suitable for handling high-speed applications in IMT-2020 systems.

4.3.3 Cognitive Radio system

The terms Cognitive radio system (CRS) are defined in [Report ITU-R SM.2152](#) as follows: “A radio system employing technology that allows the system to obtain knowledge of its operational and geographical

environment, established policies and its internal state; to dynamically and autonomously adjust its operational parameters and protocols according to its obtained knowledge in order to achieve predefined objectives; and to learn from the results obtained.” A Device using CRS would then be able to configure itself to certain radio frequencies and operating parameters taking into account reliable information available from the regulatory Authority allowing the use of these frequencies for this purpose.

A CRS generally consists of an adaptive, multiband software-defined radio (SDR, also defined in [Report ITU-R SM.2152](#)) that supports multiple air interfaces, multiple protocols, and is reconfigurable through software. An SDR contains hardware components such as mixers, filters, and amplifiers that are activated and controlled by means of software on an external computer or embedded within the radio. An adaptive radio monitors its own performance and uses closed loop actions (inclusive of machine learning capabilities) to optimize its performance by automatically selecting the appropriate frequencies and channels. These mechanisms allow it to adapt to the changes of the environment, and use available frequencies at given time and area, and use a common set of radio hardware.

ITU frameworks and cognitive radio

The Report ITU-R SM.2152-0 (09/2009)³³ defined:

- *Software-defined radio (SDR)*: A radio transmitter and/or receiver employing a technology that allows the RF operating parameters including, but not limited to, frequency range, modulation type, or output power to be set or altered by software, excluding changes to operating parameters which occur during the normal pre-installed and predetermined operation of a radio according to a system specification or standard
- *Cognitive Radio System (CRS)*: a radio system employing technology that allows the system to obtain knowledge of its operational and geographical environment, established policies and its internal state; to dynamically and autonomously adjust its operational parameters and protocols according to its obtained knowledge in order to achieve predefined objectives; and to learn from the results obtained .
- The operation of cognitive radio systems (CRS) is defined by the ITU. It shall respect the Radio Regulations (RR), the international treaty providing allocations of radio frequency bands to more than 40 defined radio services and the associated regulatory provisions for their use in a targeted interference-free environment. It shall also respect national spectrum regulations. WRC-12 considered that the current international regulatory framework can accommodate software defined radio and cognitive radio systems³⁴, by following the guidelines established on Recommendation 76 (WRC-12), “*Deployment and use of cognitive radio systems*”³⁵ recognizing that: (a) any radio system implementing CRS technology needs to operate in accordance with the provisions of the Radio Regulations; b) the use of CRS does not exempt administrations from their obligations with regard to the protection of stations of other administrations operating in accordance with the Radio Regulations . With respect to the national regulations, the RR require in particular that no transmitting station may be established or operated by a private person or by any enterprise without a license issued in an appropriate form and in

³³ Report ITU-R SM.2152 (09/2009): *Definitions of Software Defined Radio (SDR) and Cognitive Radio System (CRS)*; <http://www.itu.int/pub/R-REP-SM.2152-2009>

³⁴ Speech by ITU-R Director Francois Rancy, speech on 13 December 2013, Tunis, Tunisia, ITU Radiocommunication Seminar for Arab Countries, RRS13-Arab.

³⁵ Recommendation 76 (WRC-12): *Deployment and use of cognitive radio systems*. Radio Regulations, Edition 2012, Volume 3: Resolutions and Recommendations. <http://www.itu.int/pub/R-REG-RR-2012>

conformity with the provisions of these Regulations by or on behalf of the government of the country to which the station in question is subject (see RR No. 18.1)*. Within that international regulatory framework, it rests entirely in the hands of national regulators the decision to develop national a regulatory framework enabling the use of cognitive radio systems.

In addition to existing ITU-R publications** on this subject and to further ongoing ITU-R studies, which shall be in consistence with the Radio Regulations provisions cited above, the ITU-R and ITU-D Joint Group on WTDC Resolution 9 (Rev. Dubai, 2014), “Participation of countries, particularly developing countries, in spectrum management” is currently developing a report that will examine dynamic spectrum access approaches using cognitive radio technology based on a few recent national experiences, mainly in the UHF band, as well as the regulatory impact and challenges, and the long-term feasibility of projects using these technologies.³⁶

The most commonly used cognitive radio systems rely on geolocation databases that contain information on the location, frequency, power output, and other technical characteristics of spectrum users. Wireless devices operating on these frequencies must report their location information and then query the database for the available frequency channels and the operating parameters. Geolocation databases have been implemented and are currently operated as a part of TV white space (TVWS) systems in the United States, the United Kingdom, Canada, and Singapore.

Further, other spectrum sharing mechanism such as the Spectrum Access System (under development in the United States) and Licensed Shared Access (developed in the European Union³⁷) contemplate using geolocation databases to ensure non-interfering operation on shared frequencies. These different new regulatory frameworks are also under study within ITU-R towards providing a set of relevant solutions to national regulatory Authorities that would facilitate the share use of the spectrum and encourage its efficient use by allowing applications of different and/or similar nature to coexist in an identified spectrum environment. These different solutions may provide different level of protection and quality of service to the new service applications according to the needs.

Spectrum sensing is an alternative to the geolocation database approach, where dedicated sensors are used to measure the radio environment and enable wireless devices to commence operations on a non-interference basis. Spectrum sensing techniques have the potential to provide crucial information of the actual spectrum usage environment in specific locations as well as ensure optimum usage of the available spectrum. However, taking into account the difficulty to obtain with basic sensing equipment reliable information on incumbent users, sensing alone could not enable spectrum sharing without the support of other technologies such as geolocation databases.

* The term “licence” should be understood in its broad acceptance and means that the use of spectrum must be explicitly permitted.

** See relevant ITU-R Report in the [M series](#) and [SM series](#).

³⁶ <http://www.itu.int/net4/ITU-D/CDS/sg/rgqlist.asp?lg=1&sp=2014&rgq=D14-SG01-RES9&stg=1>

³⁷ Licensed Shared Access (LSA), Feb.2014, <http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP205.PDF>

5 Emerging and Evolving Applications

Enabled by these new technological innovations, delivery platforms, and network architectures, new classes of applications are being developed which are already having an impact on society and the economy. In many cases, these applications are built upon existing wired and wireless connectivity services – terrestrial and satellite – however enhanced platforms and architectures enable these technologies to deliver new types of capabilities. For example, Machine-to-Machine (M2M) sensors have been in use for many years. However, the varied ways in which they are now being deployed and how the data is used are anticipated to transform the way we live and work. Geospatial imagery satellites have also been in use for many years, but new ways to put this data to use are coming out of age. More importantly, the volume and expected growth of these deployments are causing policymakers across all facets of government to consider how to address a world increasingly powered by ICTs.

What are these new applications, and how are innovators finding new ways to apply technologies to address the challenges of social and economic development and build the Smart Society? How can regulators look ahead and ensure they put in place the right spectrum management, regulatory, and policy frameworks to allow these applications to flourish, encourage innovation, and stimulate investment in the economy?

5.1 Internet of Things (IoT) and Machine to Machine (M2M) – Applications for a Smart Society

Everyone has been hearing about the Internet of Things (IoT) transforming everything. Nevertheless, what does it mean and what are the technologies behind the IoT? In many cases, the connected devices that encompass M2M and the IoT are not new – in fact, telecommunications providers have been providing M2M services for many years, for example through the use of low-cost, low data-rate sensors or RFID chips in the manufacturing and fleet management sectors. The transition to the IoT involves greater innovation and interconnection of these devices, an intersection between M2M and Machine to Person applications (M2P), and improved cloud services and Big Data analytics, all intimately linked to the development of IMT-2020, common standards, and other new delivery platforms. M2M – and more broadly the Internet of Things – has been growing exponentially and the number of connected devices is forecast to be 26 billion by 2020.³⁸ This increase in volume is raising questions regarding the potential impact on society and the economy and about the policy and regulatory environment that will best enable the IoT.

The IoT has wide-ranging regulatory implications such as licensing, spectrum management, standards, competition, security, and privacy – only some of which are squarely under the mandate of telecom regulators.³⁹ Maximizing the benefits of the IoT will likely require more coordination across all sectors, with telecom/ICT regulators working closely with their counterparts in data protection and competition, but also with officials and other stakeholders in emergency services, health, highway authorities, or other sectors.⁴⁰ The sections below will address sector-specific implementations of the IoT, as well as some basic technical and regulatory considerations.

³⁸ Gartner, *Predicts 2015: The Internet of Things*, 26 January 2015, <http://www.gartner.com/newsroom/id/2970017>

³⁹ ITU and Cisco, “Harnessing the IoT for Global Development,” *Report for the UN Broadband Commission on Sustainable Development*, 2015, <https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf>

⁴⁰ Ian Brown, “Regulation and the Internet of Things”, *GSR-2015 Discussion Paper*, www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/GSR_DiscussionPaper_IoT.pdf

It is important to think of the IoT both as something new and emerging, but also recognizing that the underlying connectivity of devices to the Internet or other networks may not be new at all. Applications run across diverse wireless technologies and platforms – terrestrial and satellite, narrowband and broadband, long-range and short-range, which are already operating via existing regulatory and spectrum management frameworks.

Wireless IoT devices connect to the Internet or other networks using both unlicensed and licensed spectrum, and operate across a wide range of frequency bands, depending on requirements for the specific devices or systems. For example, IoT devices often connect via standard mobile (IMT, GSM, 4G/ LTE, etc...) and satellite (Mobile Satellite Service (MSS) and Fixed Satellite Service (FSS)) connections. Where licensed spectrum is used, regulators should examine whether existing licensing rules support – or possibly constrain – deployments of the IoT. In some cases, e.g. when new spectrum is not required and protection of existing systems is ensured, no regulatory changes may be needed since the underlying technology is the same. Short-range, low power IoT devices frequently operate using unlicensed Industrial, Scientific and Medical Bands (ISM) frequency bands, under the principle of no interference (to other radio stations)/ no protection (from other radio stations); authorized bands vary in terms of national and regional allocations (see [Report ITU-R SM.2153](#)). An example would be devices that connect using Wi-Fi, ZigBee, and Bluetooth in the 2.4 GHz or 5 GHz frequency bands. In these cases, authorizations are already in place, and developers are creating new applications using already harmonized spectrum. Wireline technologies such as fiber, DSL/copper or cable - each with varying capabilities of range, power, and bandwidth - also play a role. Global Navigation Satellite Systems (GNSS) such as GPS allows for the location services already underpinning many M2M and IoT devices.

Flexible, market-based policies for use of spectrum – implementing both licensed and unlicensed approaches – may allow for growth of these devices without a need for dedicated spectrum. One challenge will be to ensure sufficient spectrum once anticipated IoT deployments are made. The United States Federal Communications Commission’s expert IoT Working Group has predicted that the IoT will add significant load to existing Wi-Fi and 4G mobile networks. Regulators are recommended to give continuing attention to the availability of spectrum for short-range IoT communications, the capacity of backhaul networks, as well as encouraging the rollout of small-cell technology and 4G. Assuming these conditions are met, the Working Group did not expect that new spectrum authorizations will be needed specifically for IoT communications.⁴¹

Flexible licensing approaches also allow migration to new technologies possibly without the need for regulatory changes. In some cases regulators are reviewing existing spectrum frameworks to adjust rules to take account of the growth of the IoT and allow for future developments while protecting existing services. For example the UK just created a new “IoT” license in the VHF band to better clarify that this spectrum could be used for such devices, which were previously licensed more simply as “radio licenses”. Australia has also proposed changes to remove a technical barrier to the operation of narrowband low powered wireless networks in the Radiocommunications (Low Interference Potential Devices) Class Licence 2015 in the 900 MHz, 2.4 GHz band and 5.8 GHz bands.⁴²

Regulators and policymakers should also consider developing an overall IoT strategy or plan, to help take account of the broad picture of the IoT – including support for standards development, research and

⁴¹ US FCC Technological Advisory Council IoT Working Group, *Spectrum: Initial Findings, FCC TAC meeting update*, 10 June 2014, <http://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting61014/TACmeetingslides6-10-14.pdf>

⁴² Australian Communications and Media Authority, *Easier Access to Spectrum for the Internet of Things*, 15 March 2016, <http://www.acma.gov.au/Industry/Spectrum/Spectrum-planning/About-spectrum-planning/easier-access-to-spectrum-for-internet-of-things>

development, and review of issues like privacy, security, spectrum, cross border data flows or data localization requirements.

ITU and Internet of Things (IoT) Standardization

The international community has been working across diverse standards development organizations (SDO's) to agree IoT standards. Standards are important for future developments of the IoT to allow for more interoperability across devices and systems. The ITU has defined the IoT as “a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies” (Recommendation ITU-T Y.2060). In 2015, the ITU Telecommunication Standards Advisory Group (TSAG) approved the creation of Study Group 20 on the IoT and its applications, including smart cities and communities (SC&C).⁴³

ITU-T SG20 is tasked with developing international standards to enable the coordinated development of IoT technologies, including machine-to-machine communications and ubiquitous sensor networks. A central part of this study is the standardization of end-to-end architectures for the IoT, and mechanisms for the interoperability of IoT applications and datasets employed by various vertically oriented industry sectors. SG20 will assist government and industry in capitalizing on the opportunities presented by the IoT, providing a unique platform to influence the development of international IoT standards.⁴⁴

Further to the approval of [Resolution ITU-R 66](#) at the Radiocommunication Assembly RA-15 (Oct. 2015), ITU-R Study Groups are studying wireless systems and applications for the development of IoT, which may also benefit from the ITU-R studies to achieve harmonization for short-range devices ([Res. ITU-R 54](#)).

5.1.1 Smart Cities

National and local governments everywhere are racing to promote development of model ‘Smart Cities’. The UAE, Republic of Korea, the United States, and Singapore are just some examples of countries that have launched Smart City initiatives, seeking to support research and development, promote investment, and stimulate innovation in use of technology to help reduce traffic congestion, fight crime, foster economic growth, adapt to climate change, and improve the delivery of government services. While a Smart City would implement technologies broader than what is considered part of the IoT, the IoT is an integral component of the Smart City.

ITU, Smart Societies and Smart Sustainable Cities

ITU is exploring new activities related to the development of the Smart Society. ITU-D Study Group 2 Question 1/2 is examining the technologies and case studies that will help developing countries enable the “Smart Society.” Recognizing that ICTs will have a crucial role in ‘smart sustainable cities’ particularly in water, energy and waste management, and intelligent transport systems (ITS), the ITU-T established a Focus Group on Smart Sustainable Cities which concluded its work in May 2015 with the approval of 21 Technical Specifications and Reports. The FG brought together the key stakeholders – such as municipalities; academic and research institutes; non-governmental organizations (NGOs); and ICT

⁴³ ITU-T, *Focus Group on Smart, Sustainable Cities*, <http://www.itu.int/en/ITU-T/focusgroups/ssc/Pages/default.aspx>

⁴⁴ ITU-T, *Study Group 20 at a glance*, <http://www.itu.int/en/ITU-T/about/groups/Pages/sg20.aspx>

organizations, industry forums and consortia – to exchange knowledge in the interests of identifying the standardized frameworks needed to support the integration of ICT services in smart cities.

The ITU-T has adopted the following definition of a Smart Sustainable City based on the work done by the Focus Group and the United Nations Economic Commission for Europe”:

*“A smart sustainable city is an innovative city that uses information and communication technologies (ICTs) and other means to improve quality of life, efficiency of urban operation and services, and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social, environmental as well as cultural aspects”.*⁴⁵

Early Smart City initiatives offer regulators and policymakers a great opportunity to preview new and innovative technologies, support test beds for wireless innovations, build dialogue and collaboration with key stakeholders, and evaluate how current spectrum regulations and allocations will allow for a wider adoption of the Internet of Things. Spectrum and telecom regulators should evaluate current spectrum management practices, and collaborate with other Ministries and regulators who are leading on Smart City Initiatives and who have a role in identifying ICT requirements of their specific sectors. Additionally, as countries develop infrastructure such as roads, airports, bridges, and energy grids, countries may also consider how to make these “smart” through embedded sensors to take advantage of the IoT at the outset.

5.1.2 Smart Manufacturing and the Industrial Internet of Things

The manufacturing sector is one of the leading adopters of M2M and IoT applications. IoT applications have been transforming manufacturing, allowing companies to increase efficiencies, identify workforce gaps, and improve services. The Industrial Internet of Things (IIoT) will transform many industries, including manufacturing, oil and gas, agriculture, mining, transportation, and healthcare. Oxford Economics predicts that collectively, these account for nearly two-thirds of the world economy. By using sensors embedded in equipment, manufacturers can monitor systems, identify and remotely address maintenance issues, and collect data to help improve productivity. Fleet tracking can further improve the efficiency of supply chains. Industrial IoT is challenging traditional business models and forcing businesses and governments to adopt the IIoT in order to remain competitive.

Sensors and ubiquitous connectivity are behind much of the Industrial Internet of Things, with data analytics and software enabled services playing an important role in helping put the great amounts of data collected from the sensors into use. Manufacturers can use such sensors and software capabilities to support predictive maintenance, increasing efficiencies and cost savings. Additionally, agricultural companies can use this new data to calculate how many bushels of wheat can be produced on a given piece of farmland with a particular mix of seed, fertilizer, water, soil chemistry, and weather conditions. By combining analytics software with connected tractors, tillers, and planters, they can apply the precise mix of seed and fertilizer to maximize crop yield at harvest.⁴⁶

The applications of the IIoT are as varied as the industries and companies they support, and are already being implemented. How can regulators support the continued growth in use of the Internet to allow industries to remain competitive and to support, particularly in developing countries, adoption of new IoT applications? Regulators and policymakers should continue supporting communications infrastructure

⁴⁵ ITU-T, *Focus Group on Smart Sustainable Cities*, <http://www.itu.int/en/ITU-T/focusgroups/ssc/Pages/default.aspx>

⁴⁶ The World Economic Forum 2015, *Industrial Internet of Things: Unleashing the Potential of Connected Products and Services*, January 2015, http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf

development to allow for the robust and ubiquitous connectivity requirements of the IIoT. Telecommunications and ICT regulators should collaborate with industrial Ministries and regulatory authorities to ensure that existing regulations allow for the benefits of the IIoT to be realized across industries. They should also ensure that the specific ICT needs of certain sectors – like healthcare, transport or manufacturing – are addressed by ICT regulations, including measures regarding privacy and security as appropriate to enable the benefits of these technologies while protecting rights.

5.1.3 Intelligent Transportation Systems and Connected Cars

Intelligent transport systems (ITS) is a term that refers to transportation networks that fully integrates technology. ITS applications may encompass self-driving cars, connected vehicles, or smart sensors for traffic flow management. ITS can make road transportation safer, reduce environmental impact, and reduce congestion.

Both vehicle-to-vehicle and vehicle-to-infrastructure applications are being developed and deployed rapidly. BI intelligence estimates that by 2020, 75% of the cars shipped globally will have the capability to connect to the Internet, and that most of these will be through embedded connections, independent of other devices like a smartphone.⁴⁷ However, due to the lack of other supporting infrastructure and services, most vehicles globally with the capability will not be in use. In order to unlock these capabilities, then, the introduction of these new technologies needs to be well coordinated, including addressing regulatory challenges.

Work on ITS within the ITU-R was initiated in 1995, due to a significant increase in traffic on the roads, along with the growing need to integrate new technologies into land transport systems.

Spectrum, standards, and interoperability are especially important given the safety aspects of connected cars and ITS. WRC-15 agreed to two measures related to ITS. The first is the allocation of the spectrum Band 77.5-78 GHz to Radiolocation Services, in a co-primary basis, limited to short-range radar for ground-based applications, including automotive radars⁴⁸⁴⁹. This allocation provides a globally harmonized regulatory framework for automotive radar to prevent collisions, which will improve vehicular safety and reduce traffic accidents. The second measure is the adoption of the WRC-19 agenda item 1.12 on harmonizing ITS spectrum⁵⁰⁵¹. This item considers possible global or regional harmonized frequency bands, to the maximum

⁴⁷ John Greenough, "THE CONNECTED CAR REPORT: Forecasts, competing technologies, and leading manufacturers," *Business Insider*, 7 January 2016, <http://www.businessinsider.com/connected-car-forecasts-top-manufacturers-leading-car-makers-2015-3>

⁴⁸ Recommendation ITU-R M.2057-0 (02/2014): *Systems characteristics of automotive radars operating in the frequency band 76 81 GHz for intelligent transport systems applications*. <http://www.itu.int/rec/R-REC-M.2057/en>

⁴⁹ Modifications to Radio Regulations, Article 5: Frequency Allocations; decided by the WRC-15, with the addition of a new footnote: **5.559B**: *The use of the frequency band 77.5-78 GHz by the radiolocation service shall be limited to short-range radar for ground-based applications, including automotive radars. The technical characteristics of these radars are provided in the most recent version of Recommendation ITU-R M.2057. The provisions of No. 4.10 do not apply* (Final Acts WRC-15, page 51 : <http://www.itu.int/pub/R-ACT-WRC.12-2015/en>)

⁵⁰ Resolution 237 (WRC-15): Intelligent Transport Systems applications (Final Acts WRC-15, page 294 : <http://www.itu.int/pub/R-ACT-WRC.12-2015/en>)

⁵¹ Resolution 809 (WRC-15): Agenda for the 2019 World Radiocommunication Conference, item 1;12: to consider possible global or regional harmonized frequency bands, to the maximum extent possible, for the implementation of evolving Intelligent Transport Systems (ITS) under existing mobile-service allocations, in

extent possible, for the implementation of evolving ITS under existing mobile-service allocations. Since 1995, a number of Recommendations and Reports have been published to reflect the above. Most recently [Report ITU-R M.2228](#) provides characteristics, requirements and status of advanced ITS radiocommunications in various countries.

The ITU's Standardization Sector (ITU-T), in strict collaboration with ITU-R, maintains a collaboration group that is striving to create a complete, coherent, and effective package of security frameworks and standards for use within ITS communications. They are also investigating regulatory and legislative actions necessary to facilitate the deployment of ITS communication products and services based on the ITS communication standards being developed.

Ministries or departments of transportation typically lead connected-cars and ITS initiatives. Because of new technological aspects, this also requires closer cooperation with telecom/ICT ministries and regulators, as well as auto manufacturers, ICT manufacturers, and telecommunications service providers. Consideration of regulatory and spectrum requirements must also be undertaken in coordination with these multiple stakeholders both in government and in the private sector.

5.2 Unmanned Aircraft Systems (UAS)

Unmanned aircraft systems⁵² offer enormous social and economic benefits – with new commercial and non-commercial uses developed continually. Current and emerging applications for UAS include weather forecasting, 3-D mapping, precision agriculture, protection and conservation of wildlife, search and rescue, and border patrol. Companies such as Amazon.com are exploring options for using drones for delivery services. UAS can properly be seen as part of the broader ecosystem of the future Internet of Things, with drones providing another means for collecting data from remote regions, and supporting automation and efficiency within organizations. Regulatory frameworks around commercial uses of UAS are still developing, with civil aviation authorities in the lead. What pressures will the expected increase in use of UAS place on aeronautical, terrestrial, and satellite spectrum resources?

There is a wide variety in types of unmanned aircraft. There are smaller 'hobby' type aircraft; commercial line of sight operations; autonomous/unmanned systems; and remotely piloted beyond line of sight (BLOS) systems. UAS generally require spectrum for control of the device and for downlinking data collected from the device, such as video or other images. There are multiple considerations for UAS spectrum depending on the type of aircraft – whether line of sight or beyond line of sight. ITU has been studying these matters for several years, with WRC-12 agreeing on aeronautical mobile (Route) service (AM(R)S) allocations in the 5030-5091 MHz band for line of sight (LOS) and BLOS control as well as non-payload communications (CNPC). Most recently, WRC-15 agreed on the regulatory conditions and framework to pave the way for the use of commercial fixed satellite service (FSS) spectrum for UAS BLOS communications by 2023 and help ensure that the future demands for UAS BLOS spectrum can be met, while also ensuring the safety of flight⁵³.

accordance with Resolution 237 (WRC-15) (Final Acts WRC-15, page 426 : <http://www.itu.int/pub/R-ACT-WRC.12-2015/en>)

⁵² Defined by ICAO as an aircraft and its associated elements, operated without a pilot on-board. ICAO Circular 328 (2011) provides an overview of UAS in support of integration into non-segregated airspaces. <https://www.trafikstyrelsen.dk/~media/Dokumenter/05%20Luftfart/Forum/UAS%20-%20droner/ICAO%20Circular%20328%20Unmanned%20Aircraft%20Systems%20UAS.ashx>

⁵³ Resolution 155 (WRC-15): Regulatory provisions related to earth stations on board unmanned aircraft which operate with geostationary-satellite networks in the fixed-satellite service in certain frequency bands not subject to a Plan of Appendices 30, 30A and 30B for the control and non-payload communications of

Regulations and frameworks enabling UAS spectrum use for civil aviation purposes are addressed both by the ITU and ICAO internationally, as well as nationally by spectrum regulators and civil aviation authorities. There should be close collaboration among these bodies as ICAO develops international standards and national civil aviation frameworks implement them. Telecom regulations and spectrum management frameworks should also incorporate the most recent WRC decisions to allow for international development of these systems and applications.

5.3 Healthcare

ICTs have long been used to support healthcare. Telemedicine applications – for example broadband video connections – have been used to enable remote connections between patients and doctors where in person consultations are not possible.

Much like other applications, e-health and m-health applications are transforming healthcare. Wearable devices can connect patients to doctors who can monitor vital signs and address symptoms in real-time; m-health applications can be used to favorably influence patient behavior, for example by reminding them to take medications; SMS messages can support public health campaigns. Mobile applications and services can include, among other things, remote patient monitors, video conferencing, online consultations, personal healthcare devices, and wireless access to patient records.

Such applications can be particularly valuable in developing economies where access to medical services may be more limited.

The variety of applications also means a variety of spectrum resources are used to support them. Mobile networks drive many personal health applications – but systems can also rely on fixed or mobile satellite technologies for telemedicine video conferencing in remote areas. Wireless medical devices or wireless medical telemetry also rely upon both spectrum bands designated for ISM or licensed spectrum bands (by means of specific tools for monitoring devices). Regulators should collaborate with health ministries to ensure that ICT regulations are consistent with requirements of the health sector, and address potential overlapping or conflicting regulations pertaining to cross-cutting issues like security or privacy.

5.4 Geospatial Technology

Geospatial and location based services underpin much of the Internet of Things and the Smart Society. Applications like ‘friend finder’ and location marketing are important market drivers for defining and documenting the mobile Internet as well as the associated standards infrastructure enabling location-based services (LBS). More importantly, information sharing on a global basis about the natural and man-made environments is crucial to addressing humanity’s most pressing problems.⁵⁴

Geospatial technology refers to all of the technology used to acquire, manipulate, and store geographic information. These include remote sensing and earth observation satellites used to collect images from space in the Earth Exploration Satellite Service (EESS), Geographic Information Systems (GIS) or the software tools to map and analyse geographic data, GNSS (GPS) systems for determining precise locations, and other Internet mapping technologies such as Google Earth. UAS are also used to collect mapping data. Importantly, there are a number of scientific missions that collect data about the earth and the environment

unmanned aircraft systems in non-segregated airspaces (Final Acts WRC-15, page 238 :

<http://www.itu.int/pub/R-ACT-WRC.12-2015/en>

⁵⁴ ITU and Open Geospatial Consortium (OGC) ITU-T Technology Watch Report “Location Matters: Spatial standards for the Internet of Things (IoT)

http://www.itu.int/dms_pub/itu/oth/23/01/T23010000210001PDFE.pdf

and make it available for public use. Enhanced software tools help maximize value from this geospatial data. These technologies and tools offer great promise for understanding the environment and climate, predicting and responding to natural disasters, promoting good health through consumer wearables and disease outbreak mapping, or to support humanitarian aid activities.

As geospatial technologies advance, regulators should consider both the connectivity requirements, for example, to support higher bandwidth needs for higher resolution images, or the broader security and privacy considerations associated with increased collection of location data.

The ITU WRC-15 recently agreed to a new allocation in the frequency range 7 190 - 7 250 GHz to Earth-Exploration Satellite (in the path: Earth-to-space), in a co-primary basis; its use shall be limited to tracking, telemetry and command for the operation of ESS Spacecraft⁵⁵; this allocation allows to uplink large amounts of data for operations plans and dynamic spacecraft software modifications. These functions will eventually lead to simplified on-board architecture and operational concepts of spacecraft for future earth-exploration satellite services (EESS). Furthermore, WRC-15 also agreed to new allocations in the frequency ranges 9 200 – 9 300 GHz and 9 900 – 10 000 GHz to Earth-Exploration Satellite (active, i.e., radars), in a co-primary basis⁵⁶, which lead to the development of modern broadband sensing technologies and space-borne radars on active sensing EESS. Scientific and geo-information applications will provide high quality measurements in all weather conditions with enhanced applications for disaster relief and humanitarian aid, land use, and large-area coastal surveillance.⁵⁷

⁵⁵ Modifications to Radio Regulations, Article 5: Frequency Allocations; decided by the WRC-15; Final Acts WRC-15, page 5 : <http://www.itu.int/pub/R-ACT-WRC.12-2015/en>

⁵⁶ Idem 51

⁵⁷ ITU, “Press Release: World Radiocommunication Conference allocates spectrum for future innovation,” 27 November 2015, http://www.itu.int/net/pressoffice/press_releases/2015/56.aspx#.Vx4Zc3pzvOk

6 Implications for Business Models

The technological advances discussed above are having a transformative impact on business models, not just of ICT and telecommunications companies but of companies across diverse sectors. In the near term, companies of all types will form more partnerships both within and across industries as they strive to assess future demand, make strategic investments in new services, and find their place in a developing ecosystem of interconnectivity. Many new classes of companies are also finding that they have a stake in ICT and telecommunications regulation and will increasingly assert themselves in these discussions.

6.1 Greater Competition to Connect Everything

We are moving into a richer ecosystem of connectivity, in which multiple delivery platforms with different technical characteristics and capabilities will compete with one another to provide services. Though it is certain that connectivity will become omnipresent, it is not clear at this point who will play the leading role in linking the devices of the IoT together. In connecting the developing Internet of Things, businesses and customers will have many options among which to select.

The providers and operators of many types of platforms are currently jockeying to fill this role.

Mobile networks, including IMT-2020 are expected by many to carry a significant amount of this traffic. These expectations encompass many different criteria, largely but not all of which may be satisfied by IMT-2020 standards. How a IMT-2020 network would function in a future IoT ecosystem is therefore difficult to anticipate. It will doubtless have a major role to play, especially in dense urban environments, but to what extent it will predominate is not yet clear.

Satellite networks, including new geostationary high throughput satellites and low earth orbit constellations may also have an important role to play. These systems have the capability to provide global coverage in a manner no terrestrial system can and may find an important role complementing these networks. However, they may be able to do so at lower capacity than terrestrial networks and – the case of the geostationary satellites – at relatively high latency.

Traditional fiber networks, especially backbone and backhaul systems, will retain a crucially important role. Fiber is also almost certain to remain cost-prohibitive in many regions, however. The prospect of hard-wiring a large number of newly connected devices would likewise prove overly difficult and costly.

License-exempt spectrum applications they self-promote as being able to connect the largest number of devices. TVWS ventures affirm that a large portion of connections –as high as 50 percent – may be uneconomical to connect using traditional mobile networks⁵⁸ and also consider that applications like TVWS radios (discussed below) or Wi-Fi mesh networks, can be deployed more cheaply and rapidly relative to licensed mobile broadband networks, and they will be indispensable in unlocking the value of these connections. While likely necessary at small scale, these applications may not be sufficient to satisfy high data demands over longer distances. Furthermore, there are still plenty of regulatory and commercial challenges they shall firstly solve if they like to guarantee its long-term sustainability.

All of these systems will find a role to play in the IoT ecosystem, however the relative importance of each is less clear. A richer ecosystem will mean greater competition to provide services, leading to greater innovation and consumer satisfaction. Greater use of license-exempt spectrum would foster a more

⁵⁸ Richard Thanki, “The Economic Significance of License-Exempt Spectrum to the Future of the Internet,” *Microsoft Research*, 2012, http://research.microsoft.com/en-us/projects/spectrum/economic-significance-of-license-exempt-spectrum-report_thanki.pdf, p. 63.

competitive landscape for smaller players, who would not have to depend on mobile network operators (MNOs) as the gatekeepers to access customers., but long-term sustainability remains a big question for players appealing to this technical approach.

6.2 Established Telecommunications Operators Are Evolving

Traditional providers of telecommunications services face both significant challenges from greater competition, but also new opportunities as the IMT-2020 ecosystem takes shape and billions of new potential connections are available in the Internet of Things. These factors place significant pressure on established business models and will force major transformations by 2020.

Though the specific outlines of future IMT-2020 and IoT systems are not yet clear, some aspects of these systems are already apparent. They will be expected to deliver vastly greater amounts of data, connect many more devices in different ways, be more flexible in the end-to-end delivery of services, and be capable of delivering different kinds of services for different types of end-users. In meeting the technical challenges posed by these expectations, cloud infrastructure, softwarization, virtualization, and more complex network structures featuring differently sized cells all will assume key roles.

This has a number of consequences for the way operators run their businesses. Though these solutions can increase efficiencies and lower operational expenditures, they do so at the expense of higher initial capital expenditures. Capital costs are compounded by efforts that are still required to develop these technologies. Consequently, operators are already or will soon begin making large investments in these types of capabilities, and these strategic decisions will have a significant impact on their longer term performance. Regulators who want to support this process and incentivize investments in new networks need to be aware of this, and provide stable regulatory environments that give the private sector the confidence to make long term investments.

The billions of new connections that will create the IoT also offer both enormous opportunity as well as challenges to telecom operators. While the aggregate value of these connections will be enormous, the individual value of most of these connections will be quite low, making them difficult to monetize under traditional billing methods. These connected objects will increase the load on networks, but do so in different ways from traditional mobile broadband subscriptions, meaning that networks will need to adapt to different types of connectivity needs.

In the near term, many expect that competition from over-the-top services (OTT)– which may cut into traditional telecom services – will push operators towards adding value through greater

Whither MVNOs?

As the mobile telecommunications system evolves to become more service-oriented, mobile virtual network operators (MVNOs), whose model traditionally relies upon cost competition, may be under threat. As MNOs develop more data-rich services – either proprietary or in partnership with OTTs – and capital investments in new network infrastructure rise, MNOs may be less inclined to sublease their capacity. Alternatively, as MNOs develop more complex and managed core services, they may be more willing to allow smaller players to capture the basic, low-cost end of the market.

Not weighed down by legacy network infrastructure or the need for large new capital investments, mobile virtual network operators (MVNOs) may be well placed to react nimbly to market changes and develop new services. Enabled by recent advances in network architectures, some have begun to speculate regarding the development of network-as-a-Service (NaaS) or RAN-as-a-Service (RANaaS) systems which may transform the mobile network environment. In a RANaaS model, mobile network infrastructure and network access can be sold on a wholesale basis, while multiple consumer-facing services are delivered virtually through a number of different operators. If it becomes widespread, this could make the MVNO model more standard and widespread in mobile operator markets.

digital services and media offerings as well as a stronger customer experience management focus. Given the expected increase in consumption of digital streaming services, it is likely telecoms will seek to further capitalize on data-rich services enabled by the capacity. However, it is not yet clear whether the trend towards development of proprietary services will continue or whether operators will generate revenue through other methods.

The different network requirements posed by the IoT will also incentivize the development of increased B2B offerings and managed services in industry verticals. Some early estimates project that the potential value of managed services integrating back-end data analytics to be up to ten times the value of IoT data traffic alone.⁵⁹ MNOs will therefore begin to look to monetize the IoT through packages of services – at minimum for certain specialized users, if not for general subscribers, and move away from traditional data rates.

6.3 More Companies Are Now “Technology” Companies

At the same time as telecommunications providers are adapting their business models, applications of new technologies are spreading through many diverse industries. The prospect of constant connectivity, the growth in big data analytics and new computing capabilities, and the developing IoT will impact large swaths of the economy, generating new value but also new vulnerabilities and changing the nature of products and services.

As discussed above, recent advances open the door to broad new applications in sectors such as automotive, transportation, health, infrastructure, and manufacturing. While enabling new capabilities and unlocking new value, the increasing incorporation of telematics, software, and connectivity dramatically expands the scope of these companies and alters the profile of goods and services they offer. Vendors of physical goods will increasingly package their products with additional services such as cloud-based data analytics.

Durable goods and industrial equipment produced by many companies in these sectors represent significant investments and are generally expected to have a longer shelf life than the ICT products that accompany them, however. This creates an asynchrony between product life cycles, whereby the equipment may last for 20 years, but the integrated hardware and software may be obsoleted in a fraction of that time. Companies may seek to address this difficulty by making their products more reliant on upgradeable software-defined and cloud-based functionality. This may bring added versatility, but also makes such devices dependent on constant and reliable connectivity and could introduce additional security vulnerabilities.

⁵⁹ Machina Research, quoted in “Rise of the machines: Moving from hype to reality in the burgeoning market for machine-to-machine communication,” *Economist Intelligence Unit*, 2012, <http://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/f0788e6a-1ced-2f10-0eb0-ccda452468d3?overridelayout=true>

Licensing, ownership, and “Fair Repair” in the United States

The increasing integration of connectivity and software-based analytics into products may also have implications for traditional ideas of ownership. Overlapping licensing and intellectual property regimes imposed on these new products may pose challenges to an owner’s control of their property. While sale may transfer control of physical property, integrated technology may be licensed for use under restricted terms. A farmer, for example, can purchase a piece of agricultural equipment, however they are not permitted to duplicate, repair, or otherwise alter integrated software, as they may with physical components. In modern agricultural and industrial equipment, hardware and software are difficult to distinguish, and both are critical to equipment’s functioning. Agreements with telecommunications and other electronic service providers – for example to support telematics – may further limit the owners’ control.

Disputes are already beginning to arise regarding the integration of software into vehicles and agricultural equipment in a few countries. Legal action regarding the right of equipment owners to affect software modification – described by its defenders as “fair repair” – have been launched in the US, and legislative debates on the appropriateness of this right have begun in several US states.⁶⁰ This issue will only increase in importance as new classes of goods will be subject to the rights of actors besides the formal owner with power to dictate how goods are used.

6.4 More Have a Stake in ICT and Spectrum Management Discussions

With more devices connected and more data being collected, stored, and analyzed across multiple industries, new players are being confronted with policy and regulatory challenges more familiar in telecommunications and technology sectors.

An increasing number of companies will begin to find that their products and services are affected by rules governing the treatment of data traffic, including net neutrality regulations, mandated features to enable law enforcement access, and restrictions on international data transfers. Similarly, new types of products and services, as they collect, combine, and analyze more data, will need to comply with privacy and data protection standards. These aspects are increasingly relevant for new companies and expose them to different types of risks.

An array of new entities will also find that they have a stake in spectrum management discussions. As discussed above, spectrum management is already being impacted by the development of new delivery platforms. Many of these innovations are backed by technology giants such as Google and Facebook, previously concerned primarily with data and software. In order to secure regulatory approval to deploy these projects, they had to engage more deeply with spectrum management regulatory discussions.

This is also true for sectors which will deploy applications that are reliant on telecommunications services. The automotive and transportation industry, for example, is coming to understand the importance of active engagement in spectrum regulation to their future revenues as plans for autonomous vehicles, connected cars, and more advanced telematics become the norm. In the United States, for example, proposals to open frequencies long set aside for vehicle dedicated short range communications (DSRC) for other uses has forced the industry to formulate a response and engage more closely with spectrum policy processes.⁶¹

⁶⁰ “Copyright Law Restrictions on a Consumer’s Right to Repair Cars and Tractors,” *Congressional Research Service*, 18 September 2015, <http://www.crs.gov/LegalSidebar/Details/1382>

⁶¹ Auto Alliance, “LETTER TO THE ADMINISTRATION FROM V2V INDUSTRY STAKEHOLDERS,” 10 September 2015, <http://www.autoalliance.org/index.cfm?objectid=ED665740-57C1-11E5-A252000C296BA163>

Others who want to make greater use of drones, such as some retailers and logistics providers, as well as new small and amateur nanosatellite operators may soon discover the same.

Consequently, non-tech companies need to begin to grapple with these challenges and undertake proactive efforts to understand their future business interests and emerging risks in order to remain competitive. They are increasingly in need of relationships with ICT policymakers and of forward-looking engagement strategies.

6.5 New Partnerships Will Emerge to Explore New Opportunities

Use cases and future consumer demands in the IoT are unclear. Similarly, technological capabilities and standards are still evolving. Consequently, companies in various sectors are forming diverse partnerships both within and across industries in an effort to explore new perspectives, diversify their capabilities, coordinate standards, and build sector specific service offerings.

Difficult-to-anticipate market changes means that agile business models and a diverse set of capabilities in the near term will be key to adapting to future needs. To develop a greater portfolio of these capabilities and service offerings and move away from a purely capacity-based model, telecommunications providers have already begun to develop innovative partnerships. Recent examples of both inter-industry and intra-industry partnerships include: AT&T cooperating with IBM on a smart cities program, as well as with Telefónica to offer a building and home-control IoT product; Orange UK teaming up with Nespresso and Coca-Cola to launch an M2M system; India's Bharti Airtel partnering in a joint venture with the State Bank of India to develop a mobile banking app; Sweden's TeliaSonera investing in Zound Industries, a provider of electronics accessories; and Australia's Telstra investing in digital signature company DocuSign and video platform Ooyala.⁶² These deals represent the leading edge of a new wave of partnerships and collaboration as companies try to find their roles in a new ecosystem.

Partnerships will also be increasingly important to build and promote uniform standards for wider uptake of new technologies. Currently, the lack of interoperable standards is one of the primary barriers to greater update of the IoT and other technologies such as cognitive radio. National and international bodies, as well as private sector companies are often competing to establish M2M and IoT standards, hoping that theirs will become most widely adopted. While action is required to advance the issue and may confer a first-mover advantage for some, the net effect is a profusion of different protocols and standards. Consolidation of these different approaches is necessary to enable wide deployment. Several private sector consortia have been formed recently with the purpose of doing this and efforts are ongoing in international standards organizations, including the ITU.

⁶² Roman Friedrich, Steven Hall, and Bahjat El-Darwiche, "2015 Telecommunications Trends," *PWC*, 2015, <http://www.strategyand.pwc.com/perspectives/2015-telecommunications-trends>

7 Spectrum Management Considerations

The technologies discussed in this report have significant implications for spectrum management, whether directly – in the case of new technologies that require spectrum resources – or indirectly – in the case of new complementary technologies which may impact the capabilities and usage patterns of spectrum technologies. In order to begin planning future spectrum policies, regulators need to understand what tools are at their disposal to respond to changing demand. It is also important for regulators to examine whether any changes are needed not just to spectrum allocations but to their established frameworks and practices for managing these allocations. In order to adapt to change, greater flexibility of regulatory approaches and spectrum sharing solutions may be required. These considerations and other relevant challenges faced by national spectrum regulation authorities, are deeply analyzed in the recent update of ITU Handbook on National Spectrum Management (Edition 2015).⁶³

7.1 Evolving Trends

There is rising demand for spectrum resources due to the rapidly expanding application of wireless access technologies, and the spiraling increase in remotely-delivered services. Many activities – commercial and domestic – that were provided by fixed connections ten years ago are now routinely delivered wirelessly. The importance of managing spectrum efficiently is paramount in order to adapt to this rising demand.

At least three major trends are driving this increasing spectrum demand:

- **The Internet** – Twenty years ago, the Internet was a novel application of computer networking, only recently liberated from its academic roots. Ten years ago, it began changing our domestic routines as we adapted to online shopping and social networking; today it continues to reach into every aspect of our lives with the Internet of Things (IoT). What was once termed a “revolution” has become an accepted tool of communications for government, business, and domestic life, swelling in size as more and more demands are placed upon it. The ultimate strength of the Internet is the fact that it is, at heart, a simple data network that reliably conveys simple text messages on the same channel as complex entertainment – the bounds of its adaptability have not yet been reached. Because of this, it has become a significant element of the infrastructure of almost every society. Although the backbone runs predominantly across fiber-optic fixed networks, universal access to it demands increasing use of wireless technologies.
- **Mobility** – Since the spread of the mobile phone during the 1990s, businesses and consumers have increasingly expected the information and services available to them in their homes or at their desks to be accessible wherever they are. The advent of 3G networks brought an Internet access portal to our hands, and our expectations for that portal have grown with the Internet itself. Businesses are increasingly adapting to the mobility of their customers, offering dedicated services tailored for consumption on mobile devices. Even commercial shipping fleets and long-haul aircraft, as they travel to the most remote corners of the world, today routinely offer phone and internet connectivity to their crews and passengers via satellite connection.
- **Bandwidth creep** – The first wired computer networks typically operated a bandwidth of 1 Mbps; today’s wired networks typically run more than a thousand times faster. The first GSM networks offered a modest 9.6 kbps data option, compared to the heady 15 Mbps promised by today’s 4G networks. Each iteration of our communications infrastructure

⁶³ ITU Handbook on National Spectrum Management, Edition 2015; <http://www.itu.int/pub/R-HDB-21-2015>

increases the available bandwidth, but the services – and our expectations – grow at a faster rate. While most consumers were content with dial-up Internet speeds when they were browsing simple websites and sending text-only messages, they quickly demanded wireless broadband as they became familiar with multimedia messaging and video conferencing. Businesses are using video conferencing tools where a few years ago they might have simply held audio conferences. High Definition TV is quickly displacing earlier lower-resolution media.

Behind these three trends is a further inexorable force – growth in the connected population. At the end of 2015, more than 43 percent of the world’s population were connected to the Internet and the number of mobile-cellular telephone subscriptions was over 7 billion or the equivalent of 97 percent of world’s population. Twenty years ago, both of these figures were less than 1 percent⁶⁴.

7.2 Current Spectrum Management Techniques

Historically, spectrum management has been conducted on a “command and control” basis: National regulators carve-up the available radio spectrum, and license slices of it to network operators to use on highly-specific terms. Spectrum regulators have found themselves in an increasingly difficult dilemma, as more and more users demand access to spectrum, with less and less clarity on the relative merits of each proposed usage. In some cases, regulators have resorted to auctioning slices of spectrum to the highest bidder (for example, to mobile phone operators) but even this has its drawbacks – some operators have found themselves burdened with the debt from the auction, and have been unable to fully commercialize the promised network. However, this has not stopped the auction approach from being widely adopted for the most desirable spectrum. [Report ITU-R SM.2012](#) provides detailed information on the economic aspects of spectrum management.

A notable exception to licensed use of spectrum has been the rise of so-called “unlicensed” or “licence-exempt” frequency bands. “Unlicensed” does not imply the absence of a licence but actually means a general licence issued to radiocommunication devices. Most of the “unlicensed” frequency bands are used for low power or short-range radiocommunication devices (SRD)⁶⁵. They have no requirement for an individual licence since they normally use the radio spectrum on a non-interference and non-protection basis. Recently, a large number of these frequency bands have been harmonized globally or regionally in ITU administrations for common usage, and boast some of the highest and most efficient occupancy rates of any band. The most well-known is the 2400 MHz Wi-Fi band, which is accessible by virtually every broadband router, smartphone, and laptop computer in the world. Less than 90 MHz wide, it is shared every day by billions of people around the world. Three factors make this band a successful candidate for sharing: the lower power and relatively short physical propagation characteristics mean that signals in this band typically do not propagate more than a few tens of meters, limiting the potential numbers of users interfering with each other, universally harmonized frequency allocations achieved by administrations and technical standards were established and adopted by equipment manufacturers, ensuring homogenous usage.

In an effort to manage the globalization of spectrum usage more efficiently, regulators have attempted to harmonize their allocations and standards as much as possible. This can be done at the regional level with for instance the approval by European countries of relevant ECC Decisions. At the international level, this is

⁶⁴ www.itu.int/itu-d/ict

⁶⁵ [Recommendation ITU-R SM.1896 “Frequency ranges for global or regional harmonization of short-range devices”](#); and [Report ITU-R SM.2153-4 “Technical and operating parameters and spectrum use for short-range radiocommunication devices”](#).

done by the ITU WRCs with the approval of globally or regionally allocated bands to radio services (see for instance the worldwide allocations to the mobile service that are identified for IMT or automotive radars), as well as by the ITU-R study groups with the approval of ITU-R Recommendations for instance on the frequency arrangements for the implementation of the terrestrial component of IMT in bands identified for IMT in the RR.

7.3 Spectrum Management Tools

Developing an effective response to emerging technologies requires understanding not just their technical requirements, but also their likely use cases and social value. All spectrum management choices involve trade-offs. Determining which trade-offs will result in the most productive use of spectrum requires careful comparison of capabilities and potential value.

7.3.1 Flexibility

Regulators are faced with the need to critically evaluate not just what changes to spectrum allocations may be needed, but also whether their own procedures are sufficiently flexible to adapt to future needs. Historical spectrum management approaches may be too static and therefore insufficient to meet these changing needs. In addition to sometimes contributing to underutilization of spectrum resources, historical approaches of exclusive licensing can also create barriers to implementing more responsive spectrum management practices that can accommodate changing needs.

There is no single spectrum management approach or technique that will be appropriate for all countries in all contexts. However, flexible frameworks that adapt to changing needs are indispensable. Policy-makers must continually question whether historical uses of certain frequencies remain most productive, and assess whether those uses can coexist with new services and technologies. It should be recognized however that these historical approaches may still be useful to accommodate specific needs (such as for some scientific services for instances). It should be noted that [ITU-R Study Group 1](#) carries out regular studies in that respect.

7.3.2 Harmonization

Harmonizing frequency allocations – both on a regional and global level – can be an important prerequisite for the deployment of many different technologies. ITU-R “*IMT Vision*” - [Recommendation ITU-R M.2083](#),

Regulatory Challenge: striking the right balance between licensed and unlicensed approaches

The current spectrum management approach consists in establishing the right balance between licensed and unlicensed spectrum.

The current evolution of spectrum requirements calls for more sharing.

This may be done through unlicensed devices sharing with licensed users, such as RLANs sharing with meteorological radars in the 5 GHz band (since WRC-03 decision) or TVWS. It may also be done through licensed shared access (LSA).

The exclusive licensing approach through which national administrations authorize the use of frequency blocks for specific operators provides benefits in the form of security of tenure for long term investments, clarity and predictability and ease of administration at the national level.

The unlicensed approach through which globally harmonized bands are authorized by national administrations for any device compliant with essential requirements also offers benefits in the form of clarity and ease of administrations, mainly for large amounts of small investments (e.g. WiFi).

Sharing spectrum between licensed and unlicensed devices represents a challenge in that it requires a strong control of the market of unlicensed devices to ensure their compliance with the essential requirement intended to protect the licensed users. Most regulators may not have the resources to carry out this level of control.

the Recommendation R-0 (09/2015) “*Framework and overall objective for future development of IMT 2020*” recognizes that “The benefits of spectrum harmonization include: facilitating economies of scale, enabling global roaming, reducing equipment design complexity, preserving battery life, improving spectrum efficiency and potentially reducing cross border interference.”⁶⁶

Given the complex set of frequencies likely to be required for future mobile networks such as IMT-2020, technical approaches may have to assume that specific spectrum resources are not available in all countries. Emerging technologies that may be implemented based on a license-exempt regime, may also benefit from harmonization – of either available frequencies or device standards (see for instance the on-going ITU-R studies in response to [Resolution ITU-R 54](#)). Establishing device parameters that match prevailing global standards facilitate access to international markets and can help a new technology achieve greater scale, therefore reducing costs to end users. The global success of Wi-Fi is a testament to this approach.

Regulators may need to carefully examine domestic frequency allocations, and evaluate when divergence from regional or global practices is necessary to enable particular services, and when it may function as a barrier to accessing new technologies.

7.3.3 Alternatives to Device Licensing

The integration of radio equipment into new products promises to bring millions of new devices potentially within the scope of telecommunications regulations. This coming explosion in devices presents a challenge to licensing frameworks. It is impossible to license all of these devices individually and undesirable to try to do so due to the administrative burden it would place on regulators and the barriers it would present to deploying new technologies.

Rules-based and license-exempt treatment of some frequencies may be an alternative means of accommodating demand, especially for the large number of IoT connections under certain conditions, e.g. on a non-interference and non-protection basis. Such a system manages interference – either to licensed operators in those frequencies or to fellow license-exempt devices - by setting appropriate and pre-established operational parameters to be used by the license-exempt devices, which are not protected against interference from the licensed operators. This approach frees both regulators and end-users of wireless services from the burdens of individual licensing and can enable large deployments quickly. Regulators, however, still need to rule its operation through a general license (blanket license-exempt devices) fixing conditions of its use.

⁶⁶ Idem 5

7.3.4 Spectrum Sharing

As policy-makers explore ways to make use of spectrum more efficiently, spectrum sharing offers important solutions to increase the intensity of spectrum utilization. Though spectrum is finite, spectrum usage need not be zero-sum, or defined solely by exclusive blocks of frequencies.

Granting regulatory approval can be more effectively conceptualized as granting a right to use radio technologies in certain ways, defined by frequencies as well as by factors such as time period, power output, and geographic location. Depending on the needs of particular technologies, multiple uses of the same frequencies can, under the right technical and regulatory frameworks, be able to coexist effectively.

There are several potential approaches to spectrum sharing that may rely on different technical mechanisms. As such, they may be suitable for different purposes. One such technique, dynamic spectrum access (DSA), relies on cognitive radio technologies discussed above to dynamically identify and operate on unused frequencies. It can take a number of licensing forms – which range from fully licensed to license-exempt – and be deployed for many end-uses.

Some argue that dynamic spectrum access may also be an option to make more spectrum available without the long and difficult process of clearing and reallocating. Currently two major dynamic spectrum access systems are being developed or actively used internationally, usual license-exempt approach, for example for the TVWS in UHF band, and tiered access spectrum sharing mechanisms (SAS or LSA).

7.3.4.1 **Television white space (TVWS)**

Television white space (TVWS) technology is a practice to enable license-exempt sharing of unused television broadcast frequencies (VHF and UHF) in a certain area and at a certain period of time.). First tested and then ruled in the United States, regulators in the United Kingdom, Singapore, and Canada have implemented regulations to enable this technology. Several other jurisdictions including South Africa, Malawi, Ghana, the Philippines, Jamaica, and Colombia are currently exploring similar rules.

ITU spectrum sharing principles

ITU-R provides general guidance on spectrum sharing principles. “General principles and methods for sharing between radiocommunication services or between radio stations” Recommendation ITU-R SM.1132-2 (07/01))⁶⁷ describes different sharing principles including frequency, spatial, time, and signal separation techniques, and lists technical modes by which they are implemented. Revised in 2001, this recommendation is currently undergoing further revision by Working Party 1A of ITU-R in order to reflect recent changes in spectrum sharing techniques. ITU-R Working Party 1B is also studying innovative regulatory tools such as LSA to support enhanced shared use of the spectrum and the infrastructure of telecommunications network.

TVWS has received particular attention because analogue TV frequencies often have significant gaps in usage, both geographically and temporally. TV frequencies in UHF band also have particularly favorable propagation characteristics which allow them to travel long distances and penetrate walls, foliage, and other obstacles effectively. These characteristics make the frequencies especially attractive for applications such as broadband deployment in rural areas, but also increase the risk of interferences. Given the unified global allocations for VHF and UHF to the broadcasting service and the ongoing transition from analogue to digital, TVWS is promoted by its ventures to be used as a technology enabling for spectrum sharing to help bridging the digital divide in the short term. However, as mentioned before, TVWS projects are still in test phases,

⁶⁷ ITU-R, *General principles and methods for sharing between radiocommunication services or between radio stations (SM.1132)*, July 2001, <https://www.itu.int/rec/R-REC-SM.1132/en>

and their long-term sustainability has not yet proven, as key technical, regulatory and financial challenges remain unsolved.

However, according to the CEPT ECC Report⁶⁸, the White Space concept is by nature opportunistic, which implies that no guarantee can be given regarding to the availability of spectrum for use by white space devices. White space devices should be operated on a non-interference and non-protection basis and need to take into account possible future deployment of primary services in the same band and area in accordance with national spectrum policy.

7.3.4.2 Tiered Access spectrum sharing mechanisms (SAS or LSA)

Tiered access spectrum sharing mechanisms seek to enable more intensive use of spectrum by creating a system of secondary licensing. In these systems, the incumbent spectrum rights holder is generally allowed to continue its unfettered access to its licensed frequencies. Secondary licensees are allowed to access the same frequencies when and where they are not in use by the incumbent. While these secondary users can neither claim protection from nor cause interference to primary stations (current or future) they can claim protection from interference caused by other future users of the frequency band. This approach can be compared to the definitions of primary and secondary radio services having same frequency band allocated in the RR.

One example of tiered access is the Spectrum Access System (SAS) in the United States, which uses a geolocation database approach to allow three different tiers of users, each with different requirements and progressively lower levels of protection. These are the incumbent, the secondary Priority Access Licenses, and the license-exempt General Authorized Access users. The system is initially being developed to allow sharing of the 3.5 GHz band, however it may later be extended to other frequencies.

The Licensed Shared Access (LSA) system in the European Union represents another framework (see ECC Report 205). Current draft ITU-R definition for LSA is as follows: *“A regulatory approach aiming to facilitate the introduction of radiocommunication systems operated by a limited number of licensees under an individual licensing regime in a frequency band already assigned or expected to be assigned to one or more incumbent users. Under the Licensed Shared Access (LSA) approach, the additional users are authorized to use the spectrum (or part of the spectrum) in accordance with sharing rules included in their rights of use of spectrum, thereby allowing all the authorized users, including incumbents, to provide a certain Quality of Service (QoS)”*. This two-tiered system has been designed first to allow mobile broadband use in countries that wish to maintain their incumbent use in a long term in the 2.3-2.4 GHz band.

⁶⁸ Guidance for national implementation of a regulatory framework for TV WSD using geo-location databases, May 2015, <http://www.ero-docdb.dk/Docs/doc98/official/pdf/ECCREP236.PDF>

8 Considerations and Recommendations for Regulators

The regulatory treatment of new technologies requires careful consideration including whether existing regulation may already cover new technologies or applications. The cross-cutting nature of ICTs demands that regulators collaborate with other competent authorities to understand new technological deployments and how regulations will affect their use. While such increased collaboration may challenge established practice, it will also empower policy-makers with new tools to attain their goals.

8.1 Using New Technologies to Support Existing Policy Goals

The Sustainable Development Goals demonstrate that nearly all countries share the goal of extending the benefits of connectivity and information technology at an affordable cost to citizens. Governments often pursue this goal through national broadband plans, specific targets for expanding access, and comprehensive infrastructure investment plans. ICT connectivity can, in turn, also help support a wide array of policy goals in diverse areas such as healthcare, education, agriculture, financial services, or disaster response.

- **Recommendation 1:** *Policy-makers need to keep abreast of different types of technologies for delivering broadband, their costs, benefits, and technical capabilities to understand what services they may enable for citizens and how regulatory frameworks will enable, inhibit or put at risk current access to emerging technologies or continued innovation.*
- **Recommendation 2:** *National broadband plans and policies should strive for technological neutrality, to allow the deployment and future evolution of different types of services and the development of innovative business models.*
- **Recommendation 3:** *Policy-makers should consider how to take account of policy objectives in other sectors and how ICTs may support those objectives when developing frameworks for the introduction of emerging technologies.*
- **Recommendation 4:** *Policy makers should take account of best practices to promote access through new technologies, including through ITU regulations, studies and resources.*

8.2 Developing Effective Regulatory Approaches

Many emerging applications pose challenges to the traditional exercise of regulatory authority. As telecommunications regulators update outdated rules or identify whether new ones are appropriate for new applications and technologies, other regulatory bodies may also be working on frameworks to address introduction of ICTs into their sectors. Such fragmentation or overlap may pose a challenge to wide deployment and adoption of new technologies. Improved coordination across various competent authorities may help facilitate innovation and investment.

- **Recommendation 1:** *Government departments, ministries, and regulatory authorities should identify appropriate methods for collaboration and coordination on common cross-sector issues to support more effective policy and regulatory frameworks (for example, through the creation of high-level inter-ministerial working groups), taking into account the diverse stakeholders in the deployment and use of ICTs.*
- **Recommendation 2:** *Policy-makers should seek to avoid duplication of regulation to alleviate challenges from complying with differing or competing regulatory requirements.*

For further discussion of these issues, please see the GSR 2016 paper on collaborative regulation.

8.3 Creating the Environment for Investment and Innovation

The economic benefits of Internet and broadband penetration are well documented, and support economic growth, productivity gains, and development.⁶⁹ Deployment of broadband and advanced network technologies often requires high capital investments. In order to stimulate investment, countries should create an *enabling environment*. This means that regulators and policy-makers need to provide stability, predictability, and transparency regarding any regulatory requirements. Further, test beds and direct support for research and development can stimulate innovation and investment in new technologies. Such projects also allow for adaptation of new technologies to local requirements.

- **Recommendation 1:** *Support the work of ITU as well as of other globally recognized standard development organizations on international regulations, harmonization of spectrum use and standards.*
- **Recommendation 2:** *Promote and support pilot projects and test beds for new technologies, and consider incentives to promote adoption of ICTs.*
- **Recommendation 3:** *Policy-makers should create a positive and stable enabling regulatory environment – across all domains – in order to attract investment in new technologies and allow for innovation while not jeopardizing the operation and future evolution of other networks.*

8.4 Managing Spectrum Resources

Many emerging technologies rely upon spectrum. Predictions of large-scale deployments and enhanced bandwidth requirements are expected to put pressure on limited spectrum resources. Regulators will need to examine spectrum management frameworks to evaluate whether and how they may accommodate new wireless technologies without endanger current and planned radio services and stations. Increasing flexibility in spectrum management, via both licensed and unlicensed approaches, will allow for innovation and evolution of technologies and services, while balancing the needs of incumbent users.

- **Recommendation 1:** *Spectrum regulators should ensure that spectrum management practices keep pace with technology developments and that sufficient spectrum resources are available to support those that serve the public interest.*
- **Recommendation 2:** *Spectrum management should be increasingly flexible in order to accommodate (and reap the benefits of) new technologies, secure investment, stimulate innovation, and enhance spectrum efficiency, while balancing the needs of current and planned users.*
- **Recommendation 3:** *Regulators should take steps to understand current spectrum usage patterns, including through spectrum inventories, setting up spectrum observatories to measure real-time frequencies usage, and addressing any attempts at commercial or government spectrum warehousing.*
- **Recommendation 4:** *Spectrum models and rules to facilitate access as well as to minimize unused frequencies could be implemented as an important aspect of meeting demand for this finite resource*

⁶⁹ Qiang, CZW, World Bank. “IC4D: Extending Reach and Increasing Impact,” Economic Impacts of Broadband, 2009. Chapter 3 and ITU, “The impact of broadband on the economy”, 2012, <https://www.itu.int/pub/D-PREF-BB/en>

For additional discussion of spectrum management issues, see the previous GSR 2014 discussion paper on spectrum licensing.⁷⁰

8.5 Building trust and confidence

New wireless technologies and applications will enable many new connections, as well as an explosion of new means for collecting ever-increasing amounts of sometimes sensitive data. Additionally, the increased number of interconnections between devices – both wireless and wired – as well as more complex networks increase potential points of failure. Trust and confidence in new and emerging technologies is fundamental, and must be designed into the systems from the outset. Two key components to ensure trust and confidence are privacy and security.

- **Recommendation 1:** *National strategies to protect privacy must take into account a range of risks from a variety of different sources, and adapt to existing regulations.*
- **Recommendation 2:** *Regulators should stay abreast of the challenges posed by cyber threats, including the types of devices and information at risk, and their ever-changing nature.*
- **Recommendation 3:** *Addressing cybersecurity challenges requires multi-pronged approaches including: (a) strong public-private cooperation, (b) embracing international collaboration and best practices, (c) stronger domestic laws, governance systems and capacity, and (d) education efforts.*

For further discussion of these issues, please see the GSR 2016 paper on privacy and data protection.

8.6 Developing Standards

Standards are critical for broad deployment and adoption of new technologies. They assist regulators and policymakers in establishing frameworks for the marketplace that allow for interoperability and that sustain competition. They provide manufacturers an opportunity to achieve economies of scale in production that can translate into lower costs for end-users. Facilitating industry-led development of standards can be an effective approach to ensuring that standards become acceptable to major stakeholders and are best-suited to emerging technologies. The ITU has a rich history in the development of standards that are contribution-driven and consensus-based. The ITU notes with pride that in a world with over 300 bodies working on some aspect of ICT standards, they are able to provide focus, clarity and leadership.⁷¹

- **Recommendation 1:** *Regulators should avoid unique national standards for emerging technologies and should strive to promote internationally compatible standards for technology.*
- **Recommendation 2:** *Policy-makers should encourage and support industry cooperation to develop standards in addition to and in coordination with established international standards-making bodies.*

⁷⁰John Alden and Catherine Schroeder (Freedom Technologies, Inc.), “GSR Discussion paper: New frontiers in Spectrum Licensing,” *ITU-D*, 2014, http://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2014/Discussion%20papers%20and%20presentations%20-%20GSR14/Session4_GSR14-DiscussionPaper-SpectrumLicensing.pdf

⁷¹ITU-T, *FAQ: Why do we need international standards in telecommunications?*, <http://www.itu.int/net/ITU-T/info/answers.aspx?Fp=faqs.aspx&Qn=2&ewm=False>

9 Conclusions

This report has outlined some of the key changes in technology that will be affecting telecommunications and spectrum regulators in the coming years. Platforms for delivery of broadband and communications services are changing rapidly as familiar technologies improve their capacity, coverage, and technical capabilities, while entirely new systems such as IMT-2020/5G and high altitude platform stations are developed. As they compete to provide converging services, these platforms will together contribute to an ecosystem of constant connectivity.

Underpinning and enabling these technologies are significant advances in network architectures and software, including cloud computing, software defined networking, and network function virtualization. These new techniques are transforming the way that operators, particularly mobile network operators, develop and deploy their services. MNOs are discovering that technologies such as Cloud-RAN, network slicing, and heterogeneous network structures allow them to provide a higher quality of service, operate more efficiently, as well as develop and deploy services more quickly. These technologies will not only be integrated into future IMT-2020/5G networks, whose outlines will not be clear for several years, but are being deployed now to augment the capabilities of existing 3G and 4G networks which will be under strain.

As new services are developed and connectivity becomes ubiquitous, other industries are integrating new technologies. The integration of communications and data analytics capabilities into new goods creates new value for consumers and businesses, but it also exposes these businesses to new risks – including security failures – and increases their sensitivity to changes in ICT and spectrum regulation. Regulatory treatment of these goods and services frequently cuts across jurisdictional boundaries, meaning that regulatory coordination is key to creating effective frameworks. Regulators also need to be aware of and include the wide array of stakeholders that are increasingly relevant in technology and spectrum management discussions.

Changing technologies pose challenges. The increasingly interconnected and quantified world that these technologies unlock raises questions regarding how to ensure trust in their operation and what policies are most appropriate to speed their deployment. Resolving some of these questions is key to accessing the benefits of these technologies. This means that regulators must develop approaches that balance legitimate concerns and policy goals with the need to operate in a global context. These advances also place strain on both existing spectrum allocations and the ability of regulatory frameworks to adapt to rapid changes. In the near term, regulators need to undertake steps to understand how current spectrum management frameworks are suited to meet these rising challenges.

GSR-16 Discussion paper

THE RACE FOR SCALE: MARKET POWER, REGULATION AND THE APP ECONOMY

Work in progress, for discussion purposes

Comments are welcome!

Please send your comments on this paper at: gsr@itu.int by 30 May 2016



The views expressed in this paper are those of the author and do not necessarily reflect the opinions of ITU or its Membership.

CONTENTS

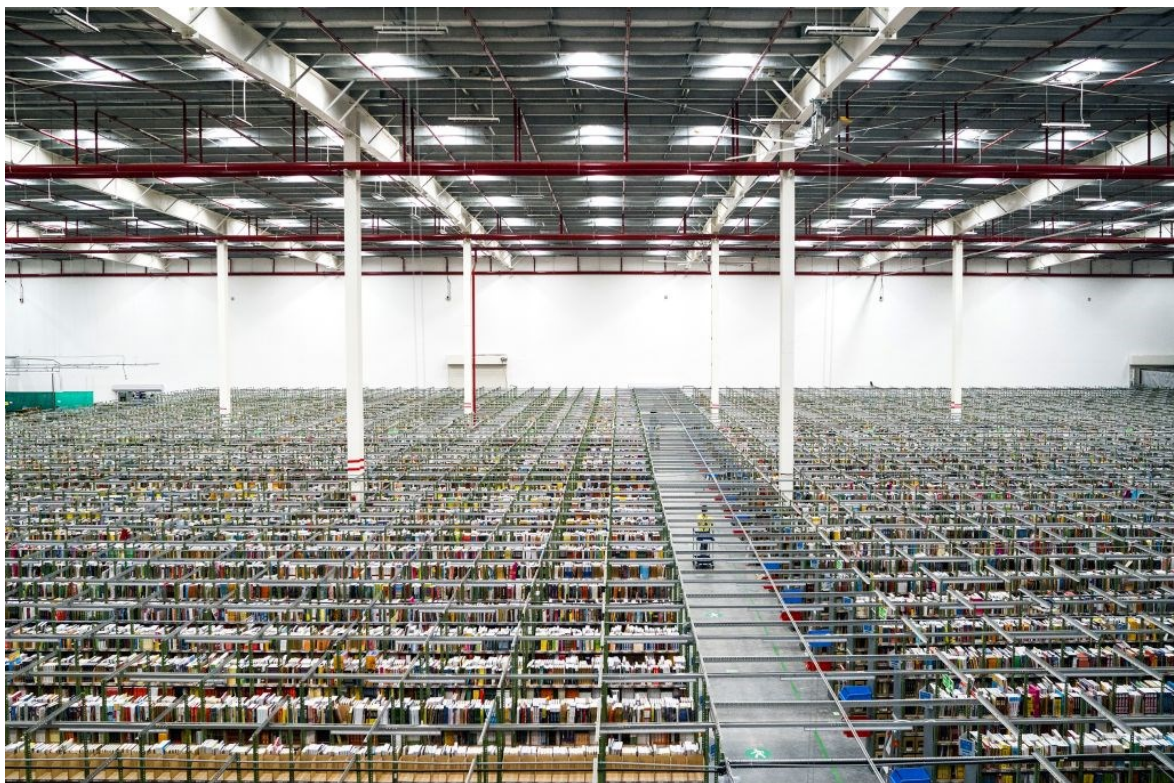
1	EXECUTIVE SUMMARY	5
2	BACKGROUND AND DEFINITION	11
2.1	What is the app economy?	11
2.2	Defining the app economy and its ecosystem.....	14
3	THE APP ECONOMY VALUE CHAIN AND THE GLOBALISATION OF APP DEVELOPMENT .	18
3.1	The structure of the app economy.....	18
4	THE ECONOMICS OF DISRUPTION.....	26
4.1	Transactions costs	26
4.2	Modes of digital disruption	27
4.3	Potential benefits of app disruption.....	31
4.4	The race for scale and the future of market power	33
5	MEASURING THE BROAD ECONOMIC IMPACTS OF THE APP ECONOMY.....	38
5.1	What is the significance of the app economy?.....	38
5.2	ICT disruption is wide-spread and ongoing: apps accelerate the process.....	38
5.3	The productivity paradox	40
5.4	Challenging traditional industry structures and definitions	42
5.5	The Value Chain and Consumer Surplus Method	43
5.6	Capital Value Method.....	47
5.7	Productivity Method	48
5.8	Value of time method	49
5.9	Commentary on potential measurement methodologies	50
6	REGULATING THE APP ECONOMY.....	51
6.1	Introduction	51
6.2	Preconditions for the development of platforms.....	53
6.3	Addressing Government, regulator and key stakeholders	54
6.4	The debate on optimal regulatory approaches.....	55
6.5	Exploring key regulatory questions for the ICT sector.....	58
6.6	Recommended approaches to regulation of the app economy	70
7	APPENDIX A: DATA FOR THE APP ECONOMY	72
7.1	Comparative global data	72
7.2	Europe.....	74
7.3	USA.....	77
7.4	Canada	80
7.5	India	82

7.6	Australia	84
7.7	Indonesia.....	87
7.8	Belarus	88
7.9	Brazil.....	89
8	APPENDIX B: THE LARGE APP ECONOMY PLAYERS	90
8.1	Introduction	90
8.2	Global Market Titans	90
8.3	Market disrupters.....	91
8.4	Regional Market Exemplars.....	92
8.5	Conclusions related to the case studies	92
	APPENDIX C: OECD BASE EROSION AND PROFIT SHARING ('BEPS') REFORMS	93
A.1	Introduction	93
A.2	Background	93
A.3	The Project	94
A.4	Final recommendations.....	94
A.5	Digital economy-specific recommendations	95
9	APPENDIX D: COMPANY CASE STUDIES	96
B.1	Introduction	96
B.2	Airbnb.....	96
B.3	Alibaba	97
B.4	Apple	99
B.5	Facebook.....	100
B.6	Flipkart	102
B.7	Google	103
B.8	iSignthis	104
B.9	LINE	105
B.10	Netflix.....	106
B.11	Skype.....	108
B.12	SocietyOne	110
B.13	Tencent	111
B.14	Uber	112

This report was prepared by ITU experts Mr Simon Molloy of System Knowledge Concepts and Mr Scott W. Minehane of Windsor Place Consulting, with significant inputs from Mr Barry Burgan, Associate Dean of Bond Business School, Bond University, Gold Coast, Australia, under the direction of the ITU/BDT Regulatory and Market Environment Division. Significant assistance was also provided by Ms Sofie Maddens, Ms Carmen Prado-Wagner and Ms Youlia Lozanova of ITU.

For this paper, the ITU experts gratefully acknowledge the assistance of a range of industry commentators. Mr Minehane also acknowledges the research undertaken of his staff at Windsor Place Consulting (www.windsor-place.com), including specifically Mr Sam Keogh, and Ms Anthea McGurty.

Amazon's 280,000-squarefoot fulfillment center in Hyderabad.



Photograph by Benjamin Lowy for Fortune Magazine (see <http://fortune.com/amazon-india-jeff-bezos/>)

1 EXECUTIVE SUMMARY

THE BIRTH OF THE APP ECONOMY

On 9 January 2007, Steve Jobs held up the new iPhone in front of the Apple faithful in the Moscone Centre, San Francisco and thereby launched the app economy. In that year, the biggest company in the world by a comfortable margin was Petrochina. ExxonMobil was next, followed by Microsoft. Microsoft was the only technology company in the top ten.

In 2015, Apple was the biggest company in the world (and had been for over two years) and Alphabet (Google), Microsoft, Amazon and Facebook jostled for other top ten positions over the year.

In 2007, Microsoft, the only pure technology company in the top ten publically traded companies, was worth 8.9 per cent of the value of the top ten. By 2015 *60 per cent* of the value of the top ten were technology companies. This is eight years of dramatic industrial change with tremendous economic and social impact. Economic transformation of this speed and scale are rare indeed.

A core element of the brief for this paper is to develop a “proposed qualitative and quantitative economic methodology to analyze the contribution of ICT digital services and apps to the economies of developed and developing countries” which will then lead to strategic dialogue and recommendations to assist policy makers and regulators to define policy frameworks and other tools for collaborative regulation to foster an enabling environment conducive to socio-economic growth, while maintaining a level playing field among all market players, promoting innovation and maximizing consumer benefits and affordable ICTs.

A NEW PHASE OF ICT DEVELOPMENT

The app economy, over the top services and the sharing economy are all new names for a set of phenomena that represent a new episode of growth of the global ICT industry. This growth is based on the rapidly approaching ubiquity of handheld computing devices, increasing wireless bandwidth, the maturation of cloud computing services and the ongoing development of mobile operating systems and their associated apps.

The app economy is best understood as a new industry or subsector of the ICT industry. For the purposes of this paper, the app economy is defined as *the sum of all economic activity, products and services, required to deliver app functionality to end users via mobile broadband services*. Until recently, this revolution has been a developed world phenomenon, but now it is well established in the developing world, primarily in China, but increasingly in India, South-East Asia, Africa, and other developing regions.

This new industry segment is itself a potentially important source of economic and social development as it creates new companies and new jobs. But potentially even more importantly in emerging economies, the widespread availability of smart devices will enable greater levels of access to a wide range of services and information that would otherwise be unachievable. This access to services and information will create new

markets and new economic opportunities and this can be expected to significantly accelerate economic development in these countries. The app economy will also drive ongoing productivity gains across all industries.

Currently, 'sharing economy' platforms often exist in regulatory grey areas operating outside the scope of the specific regulations that apply to their industry, and current competitors. Such is the speed of the broadband and smartphone revolution that collaborative business models were not anticipated by regulators, and therefore there were no applicable rules.

THE ECONOMICS OF THE APP ECONOMY

Yet, these new markets can be seen as the perfectly natural economic consequence of falling transactions costs and greater efficiencies enabled by lower cost access to information and digital services. The disruption that is occurring is driven by the same fundamental economic forces as the industrial revolution spurred by the introduction of electricity in the Twentieth Century – new technologies spur new innovation and industrial applications, business models change and new businesses and corporations displace the incumbents. The Austrian economist, Joseph Schumpeter, described this process by which new technologies and new businesses disrupt and displace old ones as 'creative destruction'.

While the development of the app economy can be characterised as a new phase in the ongoing development of ICT, it also has important distinctive elements. Because the primary consumer access point for apps is the smartphone rather than the personal computer, the app economy has far greater reach than its PC-based predecessor.

Smartphones and tablets are cheaper than computers, they are more personal and there are more of them, they have longer life batteries which means they can viably be used in emerging economy villages and recharged from unreliable electricity grids or from renewable sources – they are a more viable means of connectivity for those on low incomes. With this increased reach comes a bigger user base and this leads to an important economic characteristic of the app economy – its enormous economies of scale.

App companies are building software and hardware systems that span nations or even the globe. As each app company acquires a new user, its costs per unit fall and its competitive position improves. App companies are in a '*race for scale*' which has led (or has to the potential to lead) to a series of monopolies or near monopolies occupying various market niches. Critically, it is not only economies on the production side that drive the race for scale. App markets are also driven by *network effects*. Network effects mean that app systems become more valuable to every user when the total number of users increases – one of Facebook's greatest attraction to new users is that it has the greatest number of users. App systems such as Uber and AirBnB are more attractive to users the greater the number of drivers or rooms available, and more users attract more drivers and rooms. This is a 'virtuous circle' that drives the growth of the biggest players.

Thus, network effects can exacerbate the problems associated with market power. This is true, not only of the app players, but also true of the app ecosystem giants: Apple and

Alphabet. In these app ecosystems, more users attract more developers, which generates more apps. Since the big app players and the app ecosystem providers are globe-spanning companies, their market power challenges those of the traditional companies that they are disrupting. The geographic reach of these traditional players may be restricted to regional or national boundaries.

The sheer speed of the changes that have occurred in less than a decade has made the disruption of traditional industries very visible and it is therefore not surprising that there have been calls to protect incumbent players. It is worth emphasising that businesses in almost every industry must constantly deal with technological changes and innovation, and this ongoing process seldom generates calls for government intervention and protection against the forces of technological change. In sectors where there has been a tradition of relatively heavy regulation, however, the calls for regulatory responses are more understandable. Over time, through historical and political processes, some industries have developed quite complex and comprehensive regulatory structures that are designed, ultimately, to protect the interests of consumers and citizens. Disruptive new players tend not to be subject to such regulation and this leads to claims that the idea of a level playing field for all industry participants has been violated. This situation has created complex regulatory challenges in several industries.

MEASURING THE APP ECONOMY

If the app economy is of such significance then it is appropriate that we seek ways to measure it qualitatively. The problem is that the very characteristic that makes the app economy disruptive and significant is the same thing that makes it difficult to measure using traditional methods – it tends to undercut the relevance and usefulness of traditional definitions of industries.

The traditional approach to measuring the significance of an industry is to define the industry based on its distinctive characteristics and then to assess its size in terms of its contribution to economic activity and employment. Around the world national statistics organisations have developed processes and procedures to collect information about economic value added and employment and the resulting data collections are quite strongly grounded in traditional definitions and the historical continuity of industry structures.

The app economy creates challenges to these traditional structures by cutting across traditional industry boundaries and creating entirely new products that operate under new business models. In this report we propose methodologies by which relatively accessible data could be used to develop estimates of the size and value of the app economy.

REGULATORY IMPLICATIONS OF THE APP ECONOMY

For the digital economy to thrive, an inclusive dialogue is needed to discuss and define appropriate legal and regulatory provisions, and at the same time there is the recognition that the applicable body of law must not hamper the spread of innovation and progress within the digital economy. Regulators and policy makers must ensure consumer security, product quality and other protections in transactions, while at the same time avoiding over-regulating new collaborative business models.

While initially it may seem that the sharing economy promotes competition against legacy providers, there is a danger, as these businesses grow, that they may be tempted to exercise their own expanding market power. Competition regulators will need to be watchful that the digital economies of scale and scope are not exploited contrary to law.

The emergence of the Internet into mass markets at the end of last century and the more recent rise of the app economy are driving ICT ever deeper into the heart of all industries and sectors. Today more than ever before, a greater proportion of value is created in all businesses by the way in which they use information and communications. Increasingly business strategies are built around communications and technology strategies.

The big app and platform companies are driving a massive increase in value in the global economy. As discussed in this report, there are powerful economic and social forces at work that drive the increasing scale of these companies, particularly the niche specialists and the platform owners (primarily, Apple and Alphabet), which predispose them to increasing market power.

THE CHALLENGE TO TELECOMMUNICATIONS CARRIERS

Notwithstanding all of its newness and innovation, the primary channel from the app providers to the end consumer is the traditional telecommunications sector, with the emphasis increasingly on the mobile carriers. In emerging markets, the mobile telecommunications companies are often the only alternative, with fixed telecommunications operators being less present in these markets.

Telecommunications regulators have historically worked to limit the use of market power by fixed line and mobile carriers. They have attempted to find a balance between the level of competition and price for existing services on one hand, and the ability of carriers to earn sufficient profits to enable them to invest in quality and extent of future networks and services on the other. Regulators' efforts to optimise the short-term and long-term benefits to consumers are guided by the familiar objective of 'long term interests of end users'.

Until recently, the main economic driver of regulatory intervention has been the natural monopoly characteristics of carrier businesses, which result primarily from the physical and technical characteristics of telecommunications equipment and infrastructure. As new players emerge, the drivers of market power in the future, however, may have quite different origins.

Now the new app economy players, with their dazzling array of over the top ('OTT') services, is competing directly with the telecommunications operators, undermining consumer demand for their most profitable services, tending to commodify their outputs, threaten their margins and constrain their capacity for investment. This is happening just at the time that the app economy and OTT services are driving the demand for bandwidth ever higher.

The emergence of OTT services has sparked calls for these new players to be regulated in a similar way to telecommunications companies. The OTT players often have global scale and reach dwarfing that of the telecommunications companies, but they occupy a part of the app economy value chain that is different to the carriers and they use different input

and have different business models. The market power of app economy players arises from deep economies of scale on the 'production' side and interlocking network effects on the demand side, not, as for the traditional telecommunications companies, from the traditional natural monopoly characteristics of physical infrastructure.

The approach taken by different regulators globally to OTTs has varied thus far. However, the establishment of a 'two-track' regulatory regime for legacy telecommunication players and OTT providers in the ICT sector is also neither sustainable nor optimal.

REGULATORY CHALLENGES BEYOND THE TELECOMMUNICATIONS INDUSTRY

It is important to emphasise that the need to reconsider regulation is not restricted to the telecommunications industry. For instance, ride-sharing app company Uber is 'disrupting' the taxi business and Airbnb is doing the same to the accommodation sector. But the regulatory challenges reach beyond these specific industry boundaries. Two of the biggest areas that will require regulatory rethinking are competition policy and labour market policies.

Competition policy is designed fundamentally to protect consumer interests against the abuse of market power in a wide variety of forms. As an example, it is clear that the entry of Uber into the marketplace is increasing the level of competition in the taxi industry. Should the various local taxi companies be allowed to collaborate to develop their own app system that will compete with Uber on its own terms? Such behaviour would previously have been regarded as illegal collusion, but now perhaps it is a reasonable response to the changing competitive dynamics in the industry.

It is arguable that app systems are driving an increase in contract employment potentially at the expense of traditional employee-employer relationships. Much is made of the fact that this provides new options and flexibility for contractors¹ but these benefits need to be balanced against the potential loss in the protections for employees, especially coupled with the fact that workers may find themselves in situations where they have little choice but to seek contract work despite a preference for employment. Should governments legislate for protections to contractors; who should pay for these, tax payers or the companies that pay contractors? Clearly, the emergence of the app economy has implications for regulatory practice across multiple dimensions of the economy. Regulators that previously would have operated in relative isolation from each other will increasingly need to collaborate across industries and other domains to develop new regulatory approaches.

There are strong arguments against the establishment of a 'two-track' regulatory regime for old and new business models. Returning to consideration of the telecommunications industry, regulating fixed and mobile network operators differently from newcomers is likely to confer an unfair advantage to the model which has the least costly regulatory burden. Established business models should not be punished, relative to newcomers, for complying with regulations, nor should new businesses be punished for innovating.

¹ The Grattan Institute, Peer-to-peer pressure, Policy for the sharing economy 2016.

Harmonizing regulations between new and old businesses is desirable and arguably necessary as all industry sectors are transformed.

As part of this process of regulatory revision it will be necessary to consider explicitly and carefully the original motivations for traditional regulatory intervention and the ways in which new technologies can potentially or actually provide new mechanisms to address these original motivations. For example, the licencing of taxis and taxi drivers was motivated by the desire to protect taxi users. But new technology-enabled reputational rating mechanisms in the 'collaborative economy' provide a crowd-sourced solution to the problem of consumer protection. Examples of the operative questions that need to be addressed in shaping regulatory responses are: how effective are such mechanisms in protecting users; do these mechanisms reduce the need for oversight by regulators (at least conceptually); to what extent does reliance on these technologies predispose markets to some degree of monopolisation?

In closing, it is unlikely that any policy maker or regulator will get sharing economy regulation right on the first try. The relevant markets are still evolving rapidly and all the regulatory targets are moving. Alternative approaches that may have merit depending on the market and services concerned include temporary licensing or putting in place transition arrangements where legacy industry players are compensated for changes. The challenge is to adopt more collaborative regulatory measures where the applicable regulation on all market players is converged, coherent, promotes competition and provides incentives to invest and be innovative. A conservative approach adopting only as much regulation as is obviously necessary and giving markets the opportunity to both innovate an attempt to find solutions to meet consumer needs, would seem to have considerable merit.

2 BACKGROUND AND DEFINITION

2.1 What is the app economy?

An important first step in developing a qualitative and quantitative economic methodology to analyze the contribution of ICT digital services and apps to the economies of developed and developing countries is to clearly define “ICT digital services and apps”. Creating definitions is more complex than most people suppose. This project is not about the impact of the entire information and communications technology sector on economic and social development; it is about a subset of that sector: the app economy. For the purposes of this paper, the app economy is defined as *the sum of all economic activity, products and services, required to deliver app functionality to end users via mobile broadband services*.

The information and communication technologies (ICT) sector is an important part of modern economies and numerous studies point to the positive impact that these technologies have on economic growth both in developed and developing countries.² A new era began, however, in 2007 when Apple launched the first smartphone, the iPhone. Its new combination of features - flexible touch interface, relatively powerful processing capabilities, mobility and connectivity through mobile broadband and Wi-Fi - led rapidly to the development of new kinds of applications that have had, and continue to have, profound impacts across a range of industries and markets. Analysts found that worldwide smartphone sales in the first quarter of 2008 totalled 32.2 million units, a 29.3 percent increase from the first quarter of 2007. Vendors included Nokia, which in 2008 still commanded over 45 percent of the global smartphone market; Research in Motion, which in Q1 2010 improved its share to 13.4 percent; and Apple moved in third space in the global smartphone market with 5.3 percent share.³

A number of characteristics of the new smartphone are important. They are truly personal, unlike PCs; the fact that users generally don't share these devices means that new use patterns have emerged. The smartphone is always with you and always on – this meant that it has become ideal for a range of communications formats and notifications, including a range of reminder functions for task management. Critically, these devices are geo-aware and have an increasing number of sensors which enable the development of ever more functional apps. In addition to touch screens, increased usability and application integration, they also have powerful hardware. Apple's A9X chip, for example, today is “faster than 80 percent of the portable PCs that shipped in the last 12 months” and the iPhone 6 CPU having 625 times more transistors than a 1995 Pentium.

Smartphones are also becoming more and more ubiquitous, gradually displacing the simpler traditional voice-only mobile phones which are rapidly becoming obsolete. With

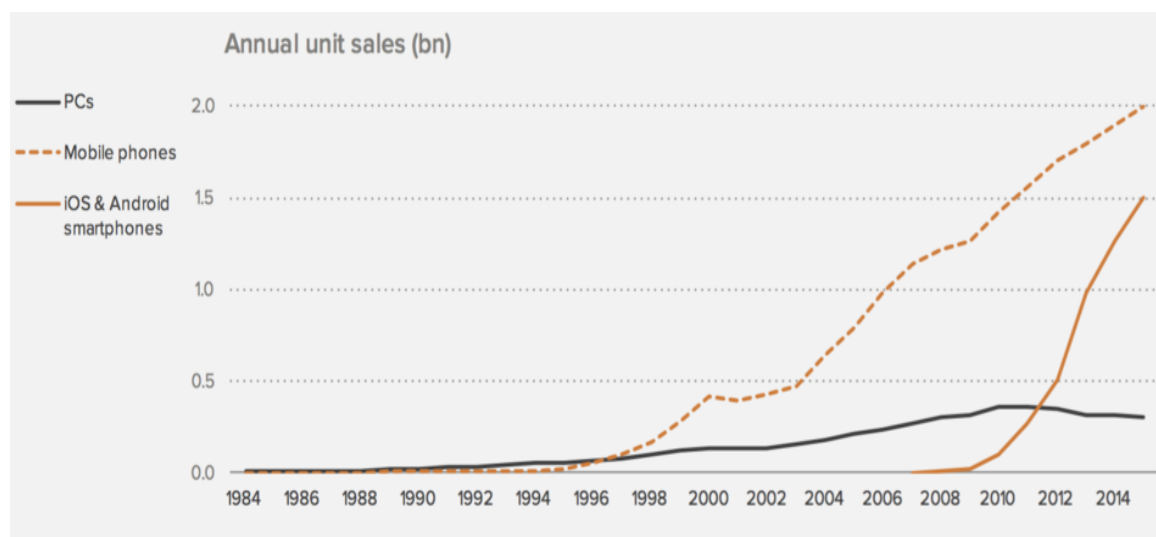
² ITU has published a number of reports focusing on Broadband issues available at <http://www.itu.int/en/ITU-D/Regulatory-Market/Pages/default.aspx>; including the last one from the Broadband Commission at <http://www.broadbandcommission.org/Documents/publications/davos-discussion-paper-jan2016.pdf>

³ <http://www.gartner.com/newsroom/id/688116>

the introduction of affordable smartphones, developing and emerging markets have been greatly increasing worldwide sales of smartphones. Studies show that in the third quarter of 2015, for example, global sales of smartphones to end users totaled 353 million units, a 15.5 percent growth over the same period in 2014.⁴ Taking into account their greater utility for consumers and their increased affordability, smartphones are set to become the world's most important and widespread consumer information and communications hardware on a global basis (See Figure 1).

Like the personal computer before it, the smartphone is also a *platform* for third party software developers. The Apple and Android app ecosystems have produced an enormous array of apps for the two main mobile platforms, with each currently containing around 1.5 million apps (see Figure 2). This has led to the development of a significant app development industry. In fact, the app economy is no more an 'economy' than, say, the television industry is an economy. It is more like a new industry, or industry subsector of the ICT industry. Like all new industries, it is, in part, displacing economic activity from previously existing industries and creating new types of products and services, just as the automobile industry did when it superseded horse-drawn transport.

Figure 1: Growing ubiquity of smartphones



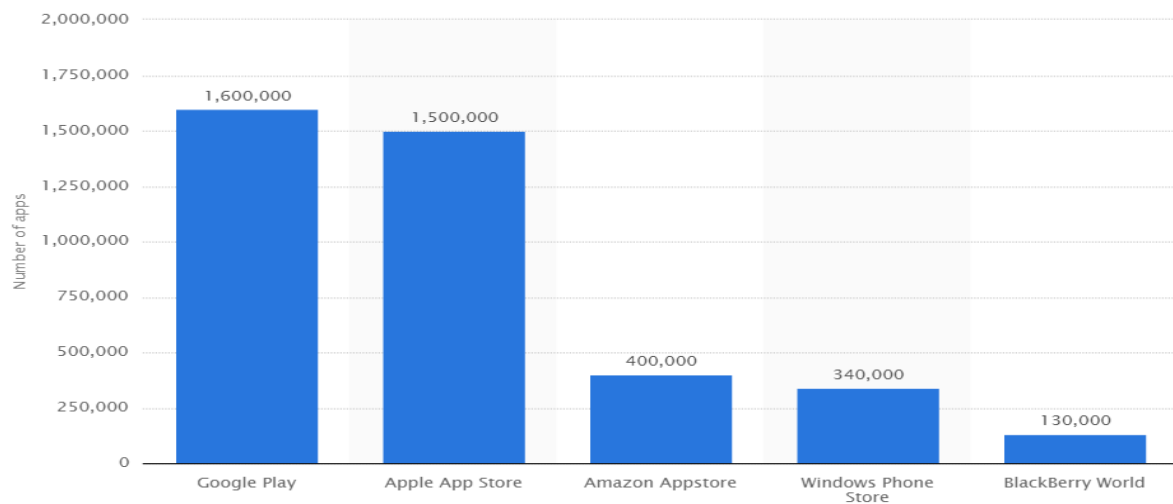
Source: Andressen Horowitz from industry sources, November 2015

In 2014, app sales revenues were USD14.3 billion and USD10 billion for the Apple and Android apps stores respectively⁵ (see Table 1). These revenues have grown rapidly with the respective figures for 2012 being USD1.3 billion and USD0.4 billion. In terms of benefits to end consumers, these revenue figures can be considered to understate economic benefits because many apps are offered free or 'lite' versions (which generate revenue from advertising or are a lead for consumers to purchase the full version).

⁴ <http://www.gartner.com/newsroom/id/3169417>

⁵ Source: www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/ (accessed 26/12/15)

Figure 2: Number of apps available in leading app stores as of July 2015



Source: www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/ (accessed 26/12/15)

Table 1: Apple and Google app store revenues 2008-15

Year	Paid to Apple (USD billion)	Paid to developers (USD billion)	Total Sales Revenue (USD billion)
July 2008 to June 2011⁶	1.07	2.5	3.57
2012⁷	1.29	3	4.29
2013⁸	3.43	8	11.43
2014⁹	4.29	10	14.29
2015¹⁰	6.3	14.7	21
Year	Paid to Google*	Paid to developers	Total Sales Revenue
2012¹¹	0.39	0.9	1.29
2013¹²	2.14	5	7.14
2014¹³	3	7	10
2015¹⁴	3.6	8.4	12

Notes: * Calculated from figures paid to developers, based on distribution of 70% of revenue to developers, 30% to Google Play (see footnotes for detail on sources).

⁶ www.engadget.com/2014/01/07/the-app-store-monster-apple-in-2013-paid-developers-more-than-d/

⁷ *ibid.*

⁸ *ibid.*

⁹ www.apple.com/pr/library/2015/01/08App-Store-Rings-in-2015-with-New-Records.html

¹⁰ <http://www.apple.com/pr/library/2016/01/06Record-Breaking-Holiday-Season-for-the-App-Store.html>; <http://www.computerworld.com/article/3019716/apple-ios/apples-cut-of-2015-app-store-revenue-tops-6b.html>

¹¹ <http://android-developers.blogspot.com.au/2015/02/a-new-way-to-promote-your-app-on-google.html>

¹² <http://bgr.com/2013/11/19/google-play-annual-revenue/>

¹³ *ibid.*

¹⁴ <http://9to5mac.com/2016/01/20/app-store-ios-downloads-vs-android-revenue/>

2.2 Defining the app economy and its ecosystem

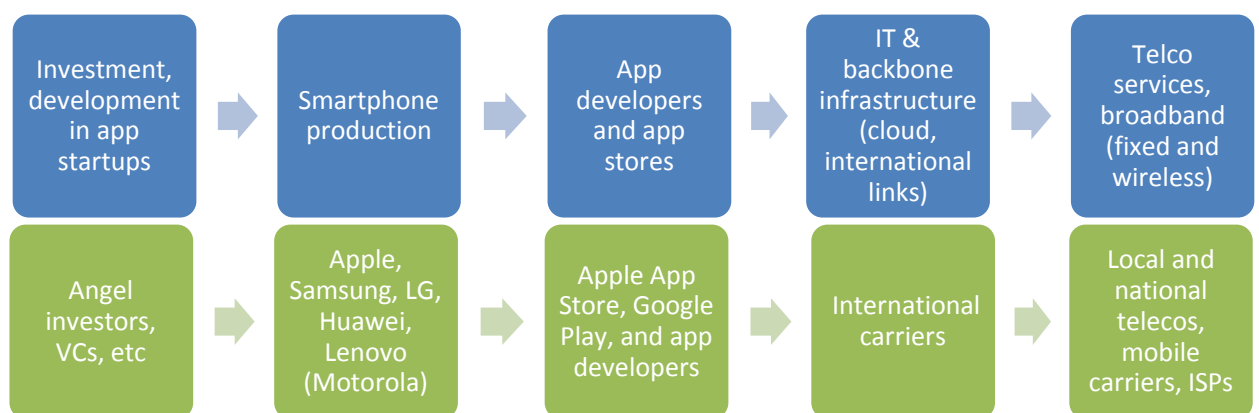
Many terms have been created over the last two decades that attempt to capture and describe the set of phenomena related to the increasing use of computers, the Internet, the web and, increasingly, the new generation of mobile devices characterised by smartphones and tablets. These include: the digital economy, the network economy, the mobile economy and more recently the terms ‘the sharing economy’, the ‘peer-to-peer’ economy and the ‘the collaborative economy’ have been coined to capture the essence of the business models employed by disruptive companies such as Uber, Airbnb, and many others.

The current wave of business disruption, which has been largely sparked by the ubiquity of smart mobile devices in advanced economies, is best understood as a continuation of the ongoing process that began with the rise of the personal computer in the 1980s and continued with the first dot com boom beginning around 1994. As such, all the various ‘economies’ identified above tend to blur into each other and creating distinct meaningful definitions is difficult.

Nonetheless, the emergence and widespread uptake of the smartphone does represent a new era in the convergence between communications and information technology, and the unique set of characteristics embodied in such devices is leading to a new wave of business disruption and creation which has no end in sight.

One starting point for developing a definition of the app economy is to understand the app value chain. In order for a consumer to have a functioning app, a number of things need to happen and various types of infrastructure and services need to be in place: the development and production of apps themselves need to be funded; smartphones need to be produced and made available at affordable prices for mass markets; well functioning app stores need to be available so that consumers can find apps and have them updated efficiently; a range of IT infrastructure and services such as cloud services need to function reliably; and, finally, broadband services, both fixed and wireless, need to be provided by telcos at prices affordable for consumers (see Figure 3).

Figure 3: App economy value chain



Source: Systems Knowledge Concepts (www.skc.net.au)

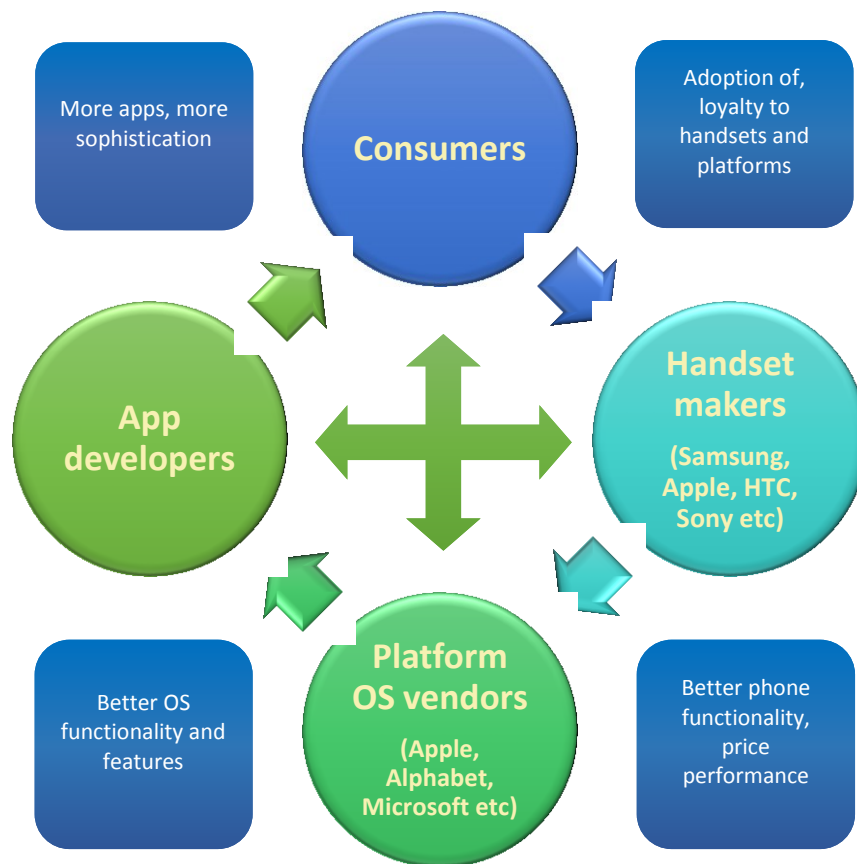
Illustrating the app economy value chain in this linear fashion, however, does not fully represent the various links and interactions between its components. Figure 4 illustrates the app economy ecosystem in terms of these interactions. Each of the major platforms needs to be sufficiently appealing to both consumers and developers. Consumers want high-quality handsets at the lowest price, a large selection of apps and operating systems with extensive feature sets. Developers want as large a market as possible of profitable consumers, high-quality development tools and to minimise problems associated with device incompatibility across the platform, which has been an issue with the various handsets running the Android OS.

The app economy ecosystem is characterised by interacting sets of network effects: the more consumers there are on a given platform, the more profitable will be app development for that platform, the more apps will be produced and the more consumers will be attracted. The manufacturers of handsets that achieved a greater scale will be able to lower unit costs, fine tune that production value chains and extract the greatest discounts from their suppliers, enabling them to be more competitive in the handset market.

Describing the app economy in this way enables us to begin to define what parts of the broader information and communications sectors could be included in the definition of the app economy. For example, telco-provided voice and SMS services would naturally be excluded from the app economy, IT back-end and cloud services not focused on supporting app functionality would be excluded and that part of the value of smartphone production that pertains simply to voice and SMS functionality should also be excluded.¹⁵ It should be immediately obvious that, while conceptually these distinctions are clear, in practice, exact data are unlikely to be available and significant estimation processes will need to be undertaken. This methodological approach will be developed further in Section 5.5 under the heading *The value chain and consumer surplus method*.

¹⁵ As should legacy feature phone production which is rapidly falling globally with Microsoft (Nokia) and Samsung the largest remaining manufacturers.

Figure 4: The 'virtuous cycle' of the app economy ecosystem



Source: Systems Knowledge Concepts Pty Ltd (www.skcn.net.au)

This discussion leads to a definition of the app economy from the value chain perspective. As mentioned above, *the app economy is the sum of all economic activity, products and services, required to deliver app functionality to end users via mobile broadband services.* This definition, as described above, includes all the economic activity in the app value chain, that is required to deliver apps and their associated network functionality to end users. Another perspective on this definition would be that it includes all the economic activity associated with producing the app platforms (primarily, IOS and Android), the apps that run on them and the Internet infrastructure, such as cloud services, that supports them. This definition should also include some services that are delivered to PCs and smart TV or set top box, for example Netflix. Netflix, a video streaming service, simply delivers a video stream that can be watched on a TV, PC, smartphone or tablet. PCs, especially laptops, are converging with tablets to some extent, and other smart devices such as TVs and even high-end digital cameras are becoming app platforms.

This definition of the app economy also highlights one of its critical characteristics from the perspective of the telecommunications industry. This is captured in another expression that is sometimes used to describe some of these new app-based services: they are said to be 'over the top' services. Services are over the top because they are made available via the generic data or broadband services provided by

telecommunications carriers. In this sense, every app is an over the top service (although this is true only in a fairly trivial sense for apps that are simply downloaded and require no further communications links once they are installed on the user device). Apps that have some type of communications or entertainment download functionality, however, represent a strategic challenge to telecommunications carriers. This is because all that users require from telecommunication companies is raw bandwidth with the value-added components being provided by the app creators. This is true whether mobile devices are using wireless bandwidth provided by mobile carriers or landline bandwidth via Wi-Fi in the domestic or work environment. Thus, the rise of apps tends to commodify telco services into simple undifferentiated bandwidth. This tends to weaken telco brand strength and potentially reduces their profitability.

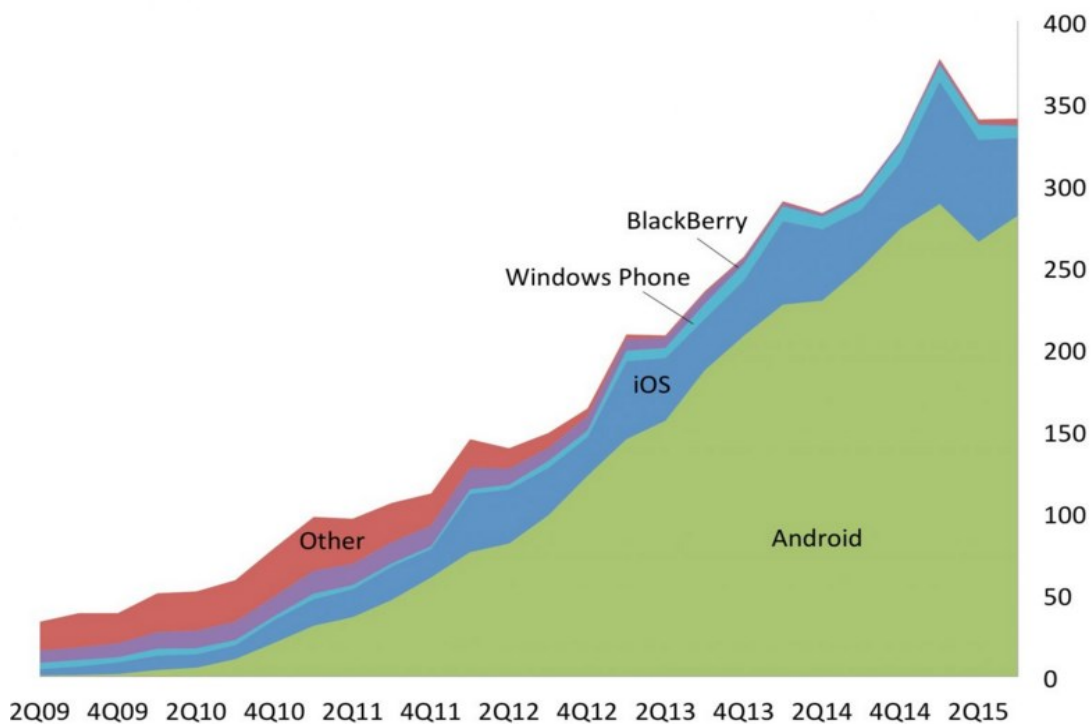
Defining the app economy to include all products and services required to deliver app functionality, including to some fixed devices such as TVs and PCs, does create some definitional and data challenges. A range of browser-based activities that use bandwidth undertaken by users on PCs and/or laptops are not part of the economy and were well-established before apps appeared and such bandwidth should, strictly speaking, be excluded from definition of the app economy. In practice, determining what proportion of the bandwidth used by a household or a business would be related to app use or not would be very difficult.

3 THE APP ECONOMY VALUE CHAIN AND THE GLOBALISATION OF APP DEVELOPMENT

3.1 The structure of the app economy

As described in the previous section, the term ‘app economy’ is a summary description of what really is a new industry or industry subsector. At the centre of this new industry there are several large and influential companies. Primary among these are Apple and Google. Figure 5 shows that Google’s Android and Apple’s iOS are by far the dominant operating systems on smartphones with Windows and BlackBerry distant third and fourth.

Figure 5: Global smartphone shipments by platform



Source: BI Intelligence <http://www.businessinsider.com.au/the-mid-year-smartphone-update-report-power-struggles-between-the-biggest-platforms-and-the-underdogs-that-are-gaining-ground-2015-9?r=US&IR=T>

Apple and Google/Alphabet follow very different strategies: Apple is essentially a hardware company that provides an operating system that is tightly bound to its hardware, whereas Google is a software company that makes an open source operating system to all hardware manufactures in order to support its search and advertising business.

For Apple, market leadership depends on the excellence of its hardware. For Google, the functionality, openness and low cost of its operating system for end users is key.

A central driver of the dominance of Apple and Google is the dominance of their app stores and app ecosystems. An app store is essentially a marketplace for app developers and app consumers within a given platform with the two main platforms being Android and iOS. While iOS is dominant in the USA and Europe, Android dominates almost everywhere else, particularly in China and emerging and developing markets.

The app ecosystem is a broader concept that includes the app stores as well as, critically, the mobile operating systems (Apples iOS and Google's Android) for each platform. It also includes the app development industry for each platform (many app developers develop for both platforms), manufacturers of handset and tablet accessories and, of course, the manufacturers of smartphones, tablets, game consoles, smart televisions and other app-capable devices.

Ultimately, the contest between platforms is driven by consumer choice. In the app economy, consumers are driven by:

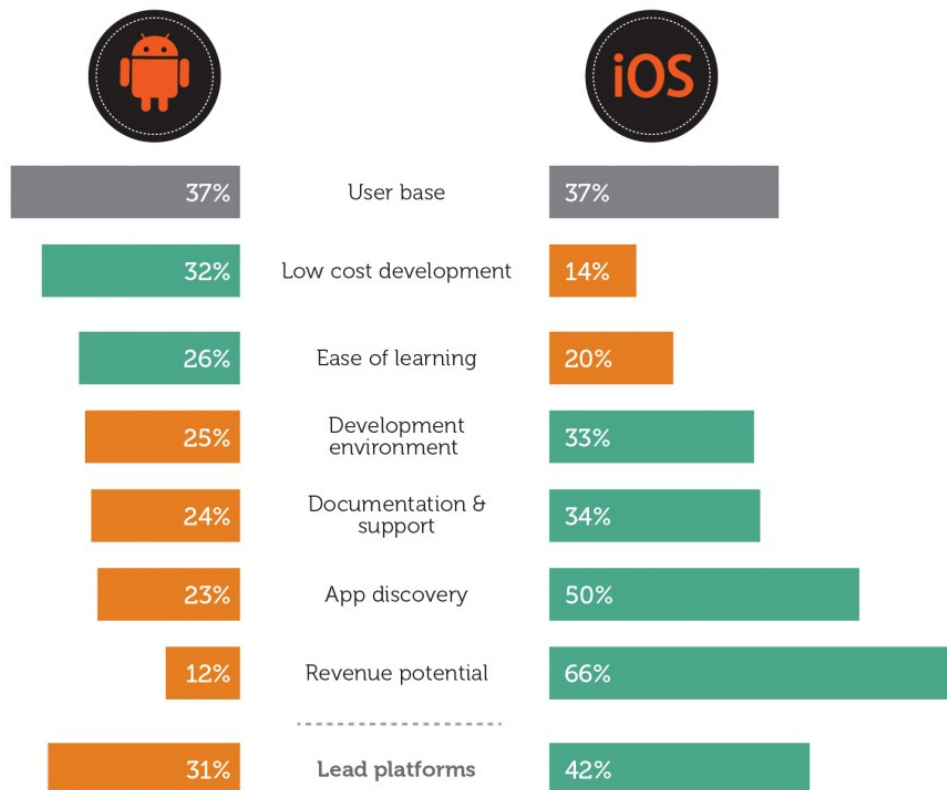
- the quality and price of hardware
- the functionality of operating systems (OS)
- the breadth of choice of apps and their quality.

Because the number and quality of apps is a critical factor driving consumer demand on each platform, the platform owners have an incentive to encourage app developers to develop for those platforms. App developers, attempting to maximise profits, will prefer the platform that enables them to sell the greatest number of apps at the highest price, sell in app purchases or monetise through advertising. Also critical will be the quality of development tools associated with each platform.

In 2013, Developer Economics conducted a survey¹⁶ of 1,200 app developers that were developing for both the Android and iOS operating systems (see Figure 6). The survey results indicated that, from a developer perspective, the two platforms have equivalent user bases but that the iOS platform created greater opportunities for revenue generation and app discovery. Apple's tightly controlled hardware and app store leads to apps being more profitable than for Android.

¹⁶ www.developereconomics.com/developer-economics-2013-survey-ios-vs-android-shoot-out/ (accessed 25/02/2016)

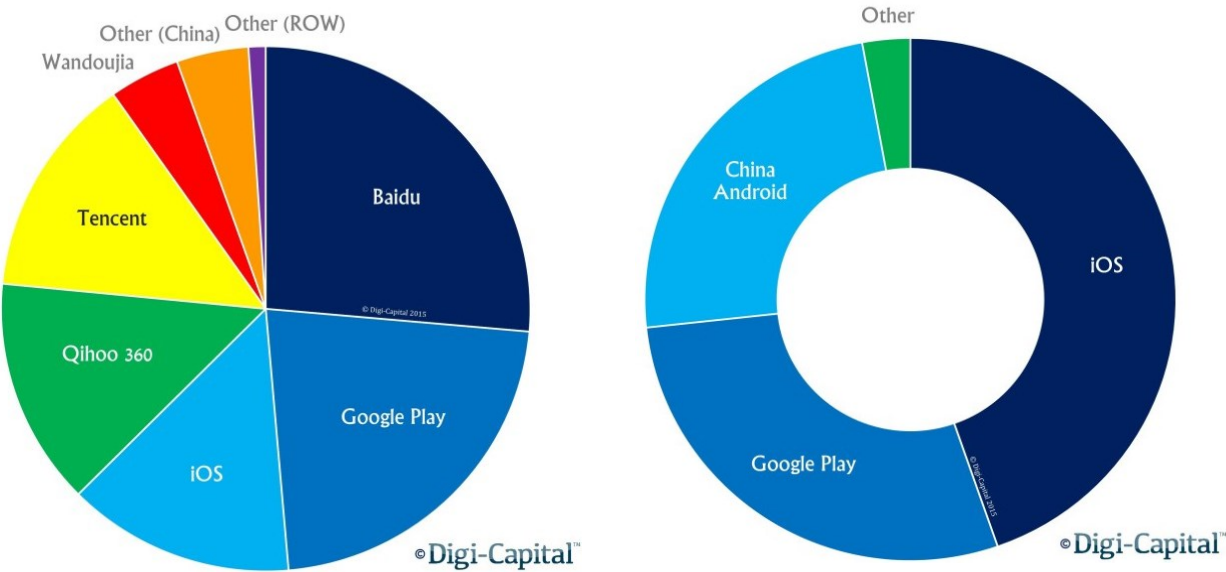
Figure 6: Android vs iOS shootout: % of developers ranking each platform top, among developers using both android and iOS



Source: Developer Economics 2013. <http://www.developereconomics.com/developer-economics-2013-survey-ios-vs-android-shoot-out/>
Licensed under Creative Commons attribution 3.0 license

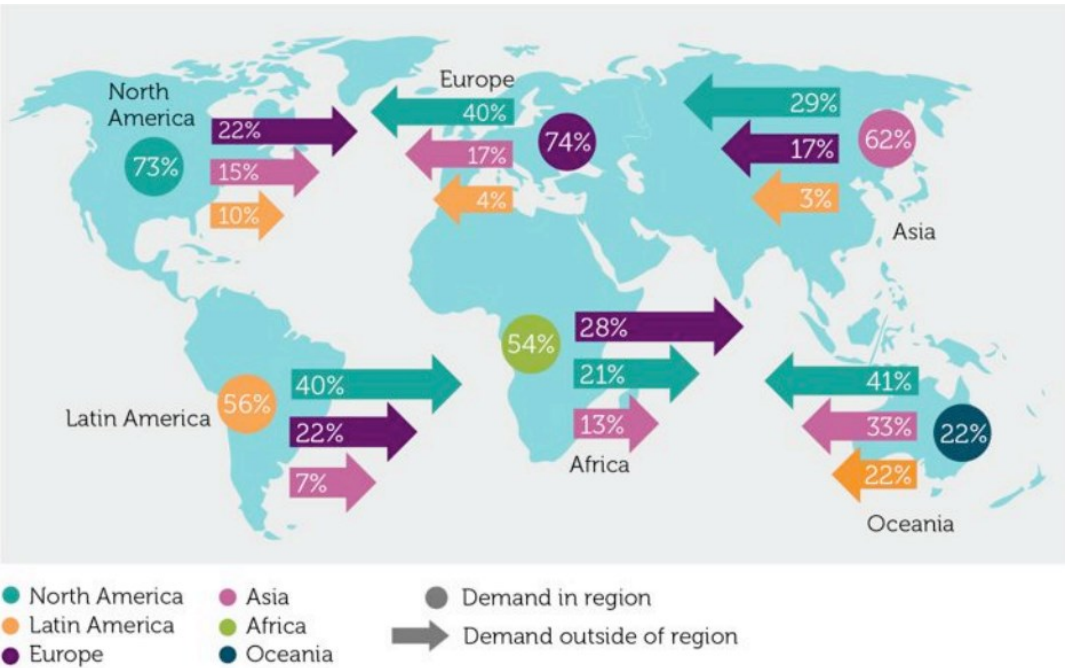
This analysis, however, largely reflects the app economy in developed countries, particularly in North America and Europe. Since 2013, the app economy phenomenon has accelerated rapidly in the developing world, for instance in India. Since Android dominates in China, Southeast Asia and India, growth in the developing world represents a growing market share for Android globally. This, however, has not meant growth for Google's App Store, Google Play because a number of Chinese companies have begun developing their own versions of Google's Android, a process that is called 'forking'. This has led to development of several large Chinese app stores such as Baidu, Qihoo 360, Tencent and Wandoujia. Figure 7 and Figure 8 show the download and revenue rankings of platforms in the increasingly internationalised app market.

Figure 7: Global app stores volume share, and by revenue value share 2014



Source: Tech Crunch <http://techcrunch.com/2015/04/27/android-surpasses-ios-in-revenue-if-chinas-android-app-stores-are-combined/>

Figure 8: Global map of app trade routes: percent of developers seeing most downloads in local versus global market

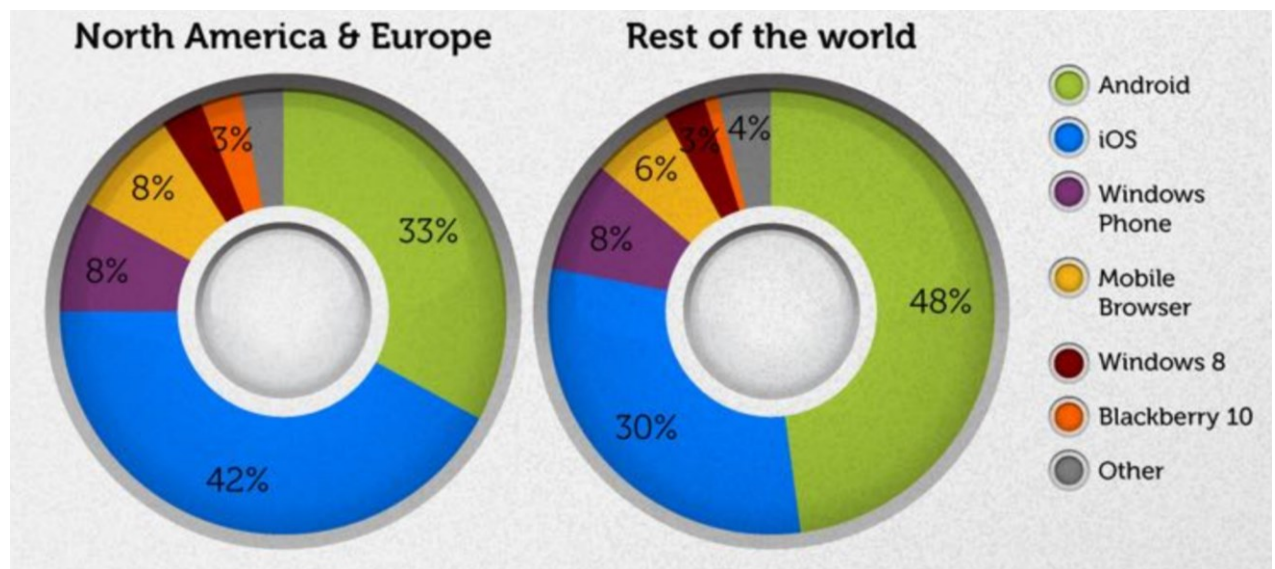


Source: Developer Economics 2012 Licensed under Creative Commons attribution 3.0 license at <https://gigaom.com/wp-content/uploads/sites/1/2012/07/screen-shot-2012-07-03-at-10-29-49-am.png>

In terms of app development, emerging trends show opportunities for developing countries in app export. A 2012 survey¹⁷ by Developer Economics shows that, while North American and European app developments were relatively highly focused on their domestic markets, developers in China, Australia, Latin America and Africa were relatively more focused on app exports.

More recently, a 2016¹⁸ study show that app developers are focusing on Android, rather than iOS, apps in most of the world outside the USA. “Even without much of the high-end, Android represents such an enormous global market that it retains 70% developer mindshare and the priority of 40% of full-time professional developers. Outside North America and Western Europe, almost half (48%) of full-time professionals are prioritising the platform and almost three quarters (74%) target it.”¹⁹

Figure 9: Percentage of full-time developer by platform by market area



Source: Developer Economics Q1 2015: State of the Developer Nation, Mobile Vision

Closely related to the app economy is the ‘start-up economy’. Like ‘the app economy’, the term ‘the start-up economy’ is also ambiguous and more of a conceptual descriptor that is attempting to emphasise the rise in the economic significance of new technology-driven companies characterised by rapid growth and disruptive business models. The economics of starting an online business have changed profoundly in the last decade - that is, since the last dot com boom. The fixed costs of starting a technology business have fallen significantly. Cloud services are now so well established and mature that new companies can buy incremental levels of service as their businesses expand, significantly

¹⁷ www.visionmobile.com/blog/2012/06/report-developer-economics-2012-the-new-app-economy/ (accessed 25/02/2016)

¹⁸ www.visionmobile.com/product/developer-economics-q1-2015-state-developer-nation/ (accessed 25/02/2016)

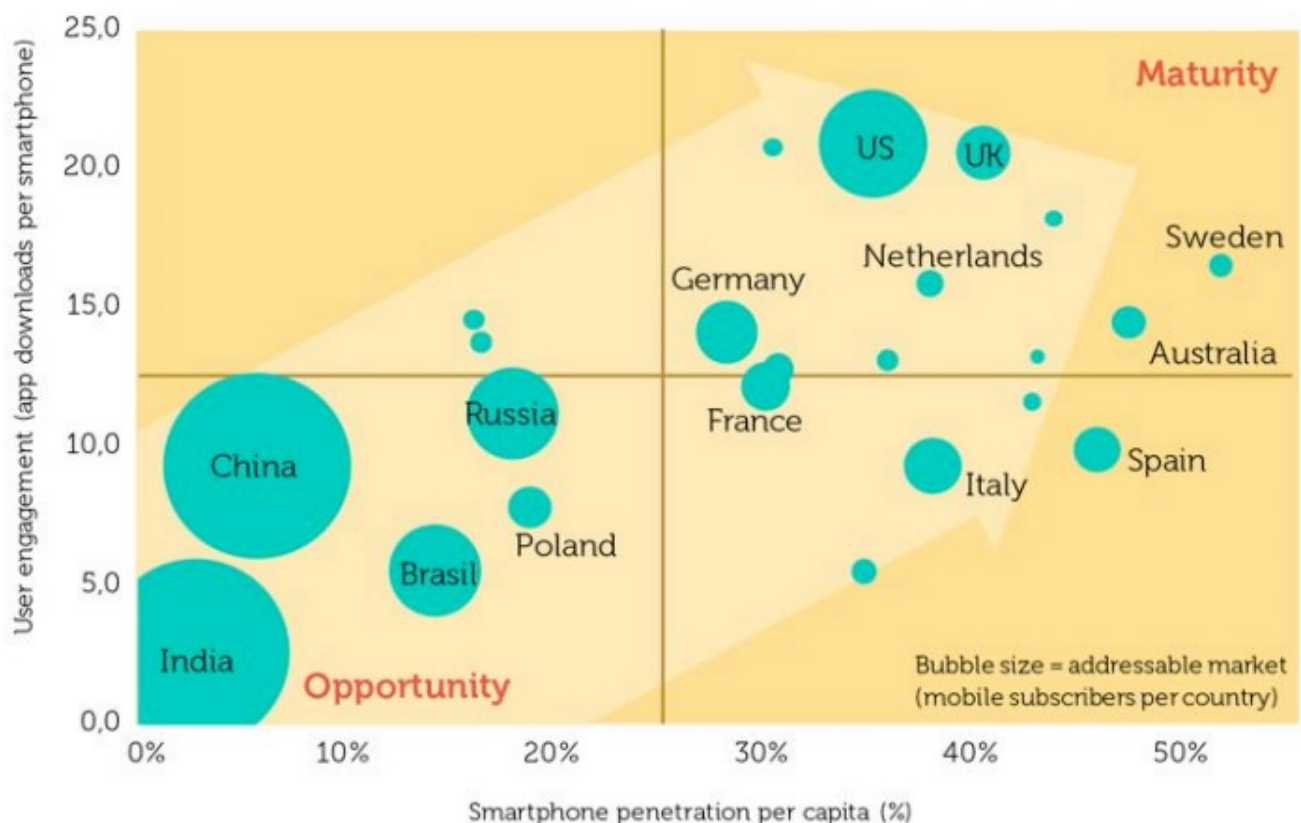
¹⁹ Ibid p 8

lowering the capital costs for start-ups. In this sense, cloud services are a critical input for the app and start-up sectors.

Companies such as Facebook, Uber and Airbnb have led more recent start-up growth in the USA. Now China has produced domestic multibillion dollar start-ups, with India close behind. In addition, budget smartphones are becoming cheaper, and consumers in developing countries will regard the smartphone as the primary means of accessing the Internet, usually through apps. As economic growth continues rapidly in China and India and smartphone penetration rapidly rises, these two countries represent an enormous opportunity for app developers.

Figure 10 shows the countries (bottom left of chart) that have potential for growth and the extent of market maturity as at 2012. As smartphone penetration per capita rises, countries with large populations and immature markets (India, China, Russia and Brazil) have the potential to greatly increase global app revenues.

Figure 10: Evolution of app demand across regions: smartphone installed base versus user engagement by country



Source: Developer Economics 2012 The new mobile app economy. www.visionmobile.com/product/developer-economics-2012/

This potential for growth is supported by a recent study (2015)²⁰ that observes that the “nationalised structure of the app stores offers an advantage to local producers in smaller markets”. The author believes, however, that this is insufficient to outweigh the winner-takes-all dynamics and platform strategies that are increasingly favoring the larger and better-resourced developers.

The dominance of the existing big app companies and of Silicon Valley as the home to the two dominant app platforms may prove to be a barrier to the growth of the app economy in developing countries. The USA, and Silicon Valley in particular, remains far and away the global centre of the app economy. Its networks, its huge community of shared knowledge in close proximity and deep risk-loving capital markets will ensure that it is not challenged in this role for the foreseeable future. The positive information externalities that characterise such economic clusters are not easily replicated.

Figure 11: Location by city of top developers (n = 2,688)



Source: <http://cariboudigital.net/wp-content/uploads/2015/04/Pon-AAG-Platforms-and-app-economy.pdf>

This means that US app companies have an advantage over the international competitors and often they will start earlier and grow faster in particular niches and, given the benefits of scale, they will be hard to catch.

At the same time, China has shown that a vibrant national app economy can develop based on the specific preferences of the domestic market. The willingness of some

²⁰ For AAG 2015 workshop on Geographies of Production in Digital Economies of Low Income Countries “Locating digital production: How platforms shape participation in the global app economy” Bryan Pon (bryan@cariboudigital.net) Caribou Digital

governments to restrict access to parts of the Internet based on internal policies has also played a part in creating opportunities for domestic app developers. Even without this particular advantage, however, app developers all over the world can build solutions that meet more local needs.

Many markets tend to be inherently local in character, example, real estate and job markets and local entrepreneurs can act on these local opportunities. Finally, it is worth observing that the history of technology companies strongly suggests that even the big app companies are vulnerable to successive waves of disruption by new and niche players.

4 THE ECONOMICS OF DISRUPTION

If the app economy had relatively little general impact on existing businesses and industries and formed self-contained niche, it would be of little interest. Clearly, this isn't the case – the app revolution is disrupting business models across many industries. One of the earliest and most spectacular examples of digital disruption was the rise of Apple to the status of the largest music retailer in the world. The Apple iPod, the iTunes Music Store and, eventually, the iPhone enabled Apple to create an entirely new process by which consumers purchase, manage and listen to music, largely displacing the CD and physical music stores.

More recently, the ridesharing application Uber has created a disruptive challenge to taxi companies all over the world, while Airbnb is providing an alternative to the traditional accommodation industry by linking individual providers of accommodation space with end users.

Not only do these developments challenge existing businesses and existing business models, they also challenge conventional classifications of the industrial structure of national economies. Whereas a traditional taxi company would have been classified as part of the transport industry, how should Uber be classified? Is it a transport company, a technology company, or some of both, or neither? Where does the power of app companies to disrupt traditional businesses come from? Are there any unifying themes or analytical frameworks that help us make sense of digital disruption?

4.1 Transactions costs

The famous 20th century economist, Ronald Coase, described the ubiquity and significance of *transactions costs* in all economic systems and how changes in these costs could lead to significant, and often counterintuitive, changes in industrial, commercial and economic structures. Transactions costs are, essentially, the costs associated with using the market to organise economic activity. A buyer must find the preferred seller; research price; research quality characteristics of the good or service that is being sought; and, if a long-term service is being sought, there is a need to design, evaluate and manage a service contract. All of these activities absorb resources.

Digital disruption: from zero to world's biggest music retailer in seven years

On April 28, 2003, Apple threw open the virtual doors to its iTunes Store, and music -- all digital media, really -- hasn't been the same since.

Suddenly, an industry terrified of online piracy had a legitimate place to earn money from the sale of digital music. Listeners no longer had to drive to their neighborhood record store (remember those?) to buy that new album by Norah Jones or 50 Cent. A song cost only 99 cents, a bargain next to an \$18 CD. And iTunes-powered iPods, with their signature white earbuds, became a must-have mobile accessory.

Not everyone was thrilled. Record labels grumbled at being strong-armed over song prices by Apple CEO Steve Jobs. Some musicians complained that they didn't earn enough royalties from digital-music sales.

But by 2010, iTunes was the largest music retailer on the planet. Today, it has 435 million registered users in 119 countries and recently served up its 25 billionth song.

Source: CNN

<http://edition.cnn.com/2013/04/26/tech/web/itunes-10th-anniversary/>

Transactions costs are often highly significant, and in some cases they may be greater than the value the buyer and seller get from the transaction itself, in which case the transaction will not proceed – in effect, the transactions costs form a barrier to the transaction occurring. Thus, high transactions costs may prevent the formation of new markets that would otherwise create benefits for both consumers and producers. In this sense, the non-formation of such markets represents a lost opportunity to create increases in what economists call ‘social welfare’. But Coase pointed out that there are alternatives to using the market to organise economic activity. Rather than using a market system, a ‘command system’ can be used. A business or a firm is, in effect, a region of economic activity within which market forces are suspended and the organisation of resources is undertaken via a hierarchical command structure. But organising activity within a business is also far from costless – the entire cost of the internal management, for example, could be characterised as such a cost. Coase described the costs of organising economic activity within a business as *organisation costs*.

The apps sector can be considered in the context of transactions and organisation costs. Improvements in technology, particularly improvements in information and communications technology, will lead to a decrease in both transactions costs and organisation costs. *Thus, the changing costs of organising activity through the market relative to the costs of doing so within the firm will drive changes to the viability of existing business models and, indeed, of new business models.* For example, within a particular industry, if transactions costs fall by more than organisation costs, then we would expect firms to shrink in size and also expect to see more activity being mediated by market processes and transactions; that is, we would expect to observe the spin-off of business divisions from parent firms and/or higher levels of outsourcing and subcontracting. The changing relative levels of transactions and organisation costs is therefore a significant driver of economic or industrial disruption.

Complicating this picture, changes in information and communications technology also lead to large changes in economies of scale meaning that businesses can operate in a particular field or market at lower per unit costs as they reach a greater scale of operation.

Once these relationships between transaction costs in the marketplace, organisation costs within the firm and economies of scale are understood, the role of technological change in the process of business and industrial disruption can be more easily understood in a more systematic manner.

4.2 Modes of digital disruption

Within the conceptual framework of transactions costs, organisation costs and economies of scale, digital disruption may take a number of forms. These are discussed below.

4.2.1 Falling transactions costs creating new markets

Prior to the development of the Web and the app economy, it would have been *technically* possible to create a business that kept centralised records of spare accommodation in domestic residences around the world that manually collected and maintained ratings for these properties and matched these with requests for such accommodation. Similarly, it would have been possible for any individual to call at random domestic residences at a particular holiday destination and attempt to negotiate an agreement for temporary accommodation. In the former case the organisation costs, and in the latter case the transactions costs, were prohibitively high and such a market simply did not develop (at least not to the extent that it more recently has).

As an example, Airbnb's business innovation was to develop a scalable information technology system that enabled the registration of available space, a rating system for providers and users and pro forma processes for reducing the costs of negotiation and payment. In effect, Airbnb used information technology to create a marketplace with massively lower transactions costs and the significant investment for this system development is now amortised on a global basis leading to relatively low unit organisation costs.

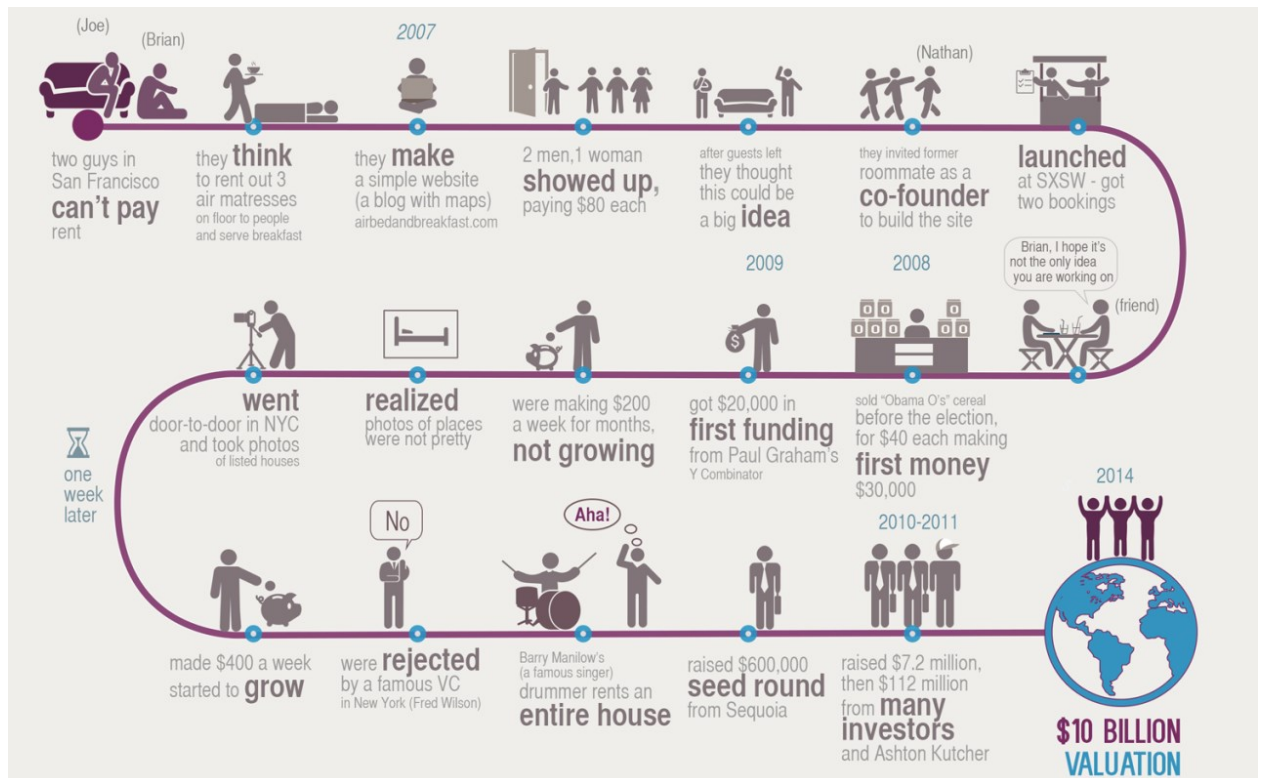
Much of the technology deployed by the disruptive app companies is designed precisely to reduce transactions costs in this manner. Through a combination of websites, mobile apps and back-end software, a new marketplace is formed where sellers can place offers and buyers can access them. Such processes massively decrease the information search components of transactions costs – something that was previously only technically possible thus becomes commercially feasible as well.

The various rules and procedures associated with these systems (for example, registration of credit card details to establish identity and various 'reputation ratings systems' such as those pioneered by eBay) provide an environment where buyers and sellers feel confident enough to trade. The terms governing use of these applications significantly reduce the 'policing and enforcement' aspects of transactions costs.

Figure 12 shows the process by which Airbnb developed from 'an idea' to a company valued at \$10 billion. It should be emphasised, however, that in addition to the total of \$2.4 billion investment in the company over multiple rounds²¹, such businesses are only possible because of the 'accumulated infrastructure' of the app economy that includes the major platform operating systems, the installed base of smartphones in use, the infrastructure of the Internet and telecommunications system, and the ongoing provision of sufficient reliable network access and bandwidth by telcos and ISPs. Together, these investments, ideas and services make possible the development of new markets based on vastly reduced transactions costs, deep specialisations and technological innovations.

²¹ https://en.wikipedia.org/wiki/Timeline_of_Airbnb (accessed 25/02/2016)

Figure 12: How Airbnb started: or how 3 guys went from renting air mattresses to a USD10 billion-dollar company



Source: Funders and Founders (based on reports in Telegraph, WSJ and The Atlantic)

4.2.2 Retailing 'information rich' products and the benefit of scale

Using scalable information technology systems, Apple was able to grow rapidly to become the world's biggest music distributor and Amazon did the same thing for books. Music and books are both complex 'information rich' products – it is difficult to evaluate the benefit they deliver until they are consumed. Consumers wish to discover new works that interest them and, because these goods are complex and there are many of them, they face relatively high transactions costs in finding what they want.

Apple and Amazon have developed large and complex retail information systems that are globally scalable and significantly reduce these transactions and operational costs. These systems enable such companies to specialise, on a global basis, on a particular type of retailing, displacing traditional bricks and mortar stores (Tower Records, which opened in 1968, and was the biggest music retailer in the USA, closed in 2006²² and the Borders Group which operated 511 superstores in the US in 2010, closed its last stores in September 2011²³).

²² www.theguardian.com/business/2006/oct/09/retail.usnews (accessed 27/12/2015)

²³ <http://www.annarbor.com/business-review/borders-liquidation-chapter-11-ann-arbor-bookstore-chain-borders-group-e-books/> (accessed 06/03/2016)

Once these systems are set up and as they are improved over time, there is no limit to their scale – they become global shopping spaces. Because economies of scale are so significant, smaller firms will tend to fail and larger firms grow, leading to the potential for globe-spanning monopolies to develop. Within this context there will be smaller niche and local players.

4.2.3 ‘Excising’ the information component of traditional businesses

The rise of Uber, for instance, graphically illustrates how app economy entrepreneurs seek out the information components of traditional businesses and launch disruptive applications.

To consider the example of Uber further, it is useful to think of traditional taxi companies as being made up of two components – the physical and the information components:

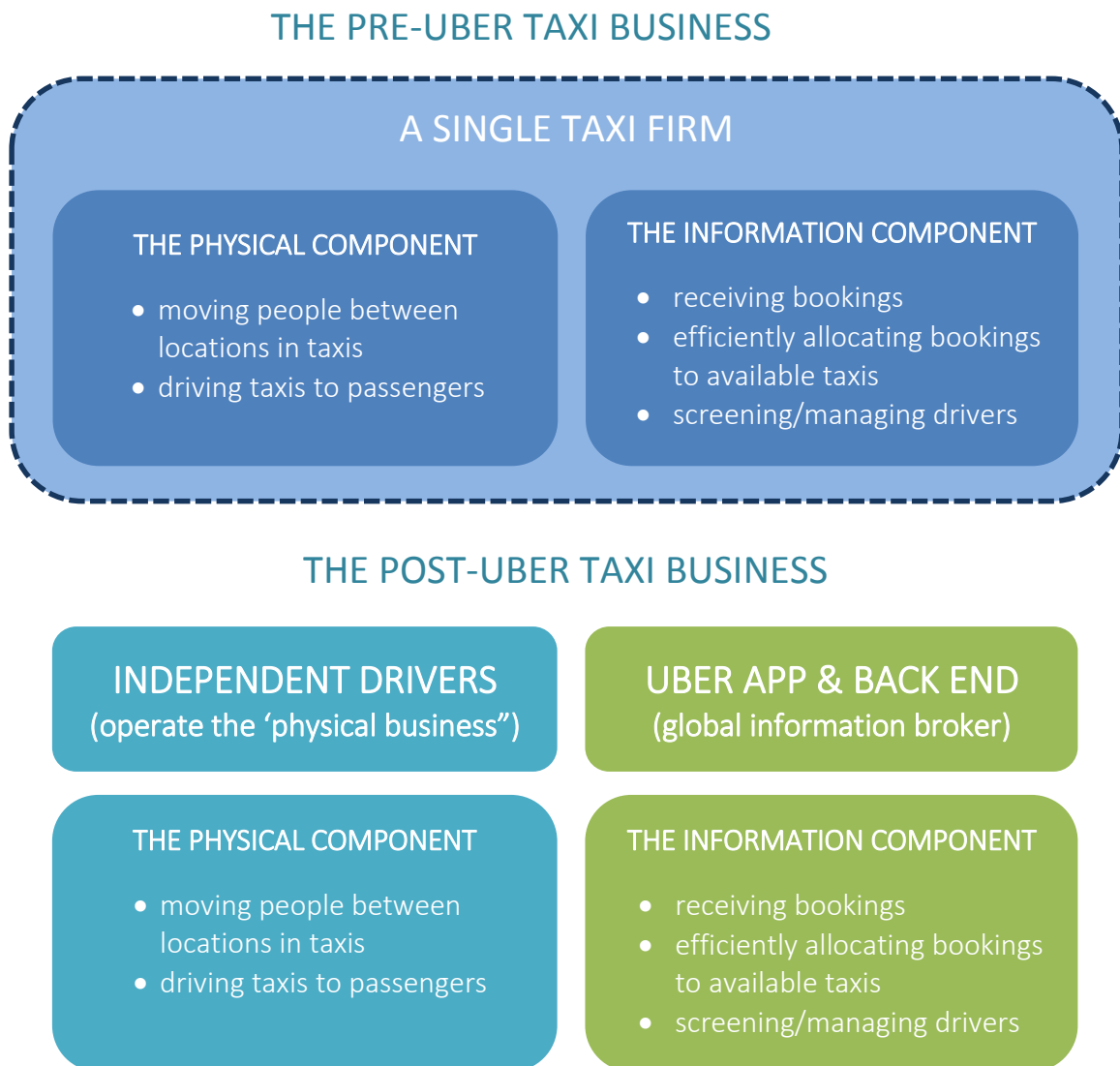
- the physical component is moving taxis to where passengers are and moving passengers in taxis to their destinations – both of these things involve the movement of physical objects through geographic space
- the information component is receiving incoming requests for taxis, coordinating these requests with available taxis, advising taxi users of taxi availability, dispatching taxis and managing a roster of drivers – these require the movement of information between the users of this information.

Traditionally, these two parts of the taxi business have resided within local taxi businesses that operate in all major cities of the world. Uber has worked out how to carve out or ‘excise’ the information component of the taxi business.

Uber and other ridesharing applications provide an alternative means for organising and operating the information component of the taxi business. Figure 13 illustrates how Uber offers a disruptive new processes by which customers and drivers, who both carry GPS capable smart devices, interact with Uber’s distributed broking software to generate automated efficient solutions that replace human dispatchers in the traditional taxi business.

Because the basic problem of taxi-passenger geo-coordination and taxi dispatching is similar all over the globe, Uber can use its application and back-end server infrastructure anywhere in the world where GPS signals are available to use with handheld consumer devices.

Figure 13: Disrupting the taxi business



Source: Systems Knowledge Concepts Pty Ltd (www.skcn.net.au)

Uber's innovations have enabled processes that previously operated inside firms, to be taken outside into a newly created app-based marketplace. Uber's systems, by harnessing the capabilities of modern mobile operating systems, can provide enhanced services to users, such as accurate wait times and live map readouts of approaching taxis. Uber has also introduced demand-responsive pricing for ride services, which arguably results in more efficient operation than traditional business models can provide by better matching global demand and supply.

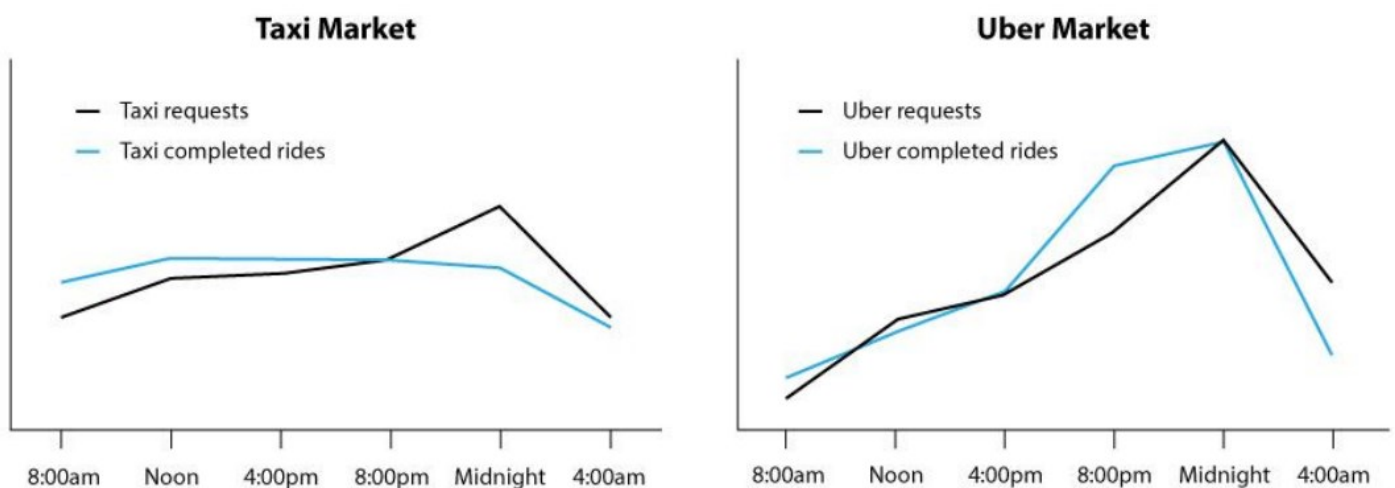
4.3 Potential benefits of app disruption

Economists use the term 'social welfare' to describe the overall benefit to society from all economic activity and government policy settings. Thus, the desirability of a particular economic change or policy change can be assessed in terms of its impact on social welfare.

By reducing transactions costs and creating markets, new technologies and applications enable buyers and sellers to come together more cheaply than previously possible. In general, assuming markets are working well, well-informed trade motivated by mutual advantage is thought by economists to unambiguously increase social welfare. But these new applications can do more than just bring buyers and sellers together. They can, for example, more easily accommodate dynamic pricing. Simply put, dynamic pricing is designed to achieve better matching of supply and demand. In the case of taxis, clearly there are periods of very high demand and very low demand. Traditional taxi drivers do have an incentive to increase supply during periods of high demand because on average they will spend more of that time with passengers at these times.

In the case of Uber, periods of peak demand are associated with higher prices so that drivers have a double incentive to increase aggregate supply at the busiest times. Figure 14 shows in black the level of taxi requests per unit time across the day and in blue shows the number of completed rides for both traditional taxis and Uber. Under Uber's system of dynamic pricing, completed rides much more closely matched demand.

Figure 14: Uber versus Taxi Supply and Demand in Austin, USA, 2014



Source: Ryan, 'Providing rides when they are most needed,' Uber Blog, September 13 2014, <http://blog.uber.com/atxsaferides>, in How over-regulation could destroy an economic revolution: The sharing economy, The Institute of Public Affairs December, 2014

Decreasing transactions costs also enable higher utilisation of existing resources such as Airbnb's use of spare rooms and houses. Other apps enable users to share power tools, boats or cars.

It should be recognised, however, that advocates of the app economy or the sharing economy emphasise the positive dimensions. But not all of these benefits are achieved without associated costs. For example, increasing utilisation means increased wear and tear and shorter operational life for capital assets. Further, the various reputational mechanisms employed do not eliminate all risks to participants. One of the characteristic objections of existing players that are experiencing disruption is that they bear the costs of traditional regulatory imposts that are designed to protect consumers.

As well as business disruption, therefore, such innovations also create regulatory disruption and regulatory responses by authorities, and play a large role in determining the success or otherwise of these new app-based corporations. The taxi industry is heavily regulated for good reasons, primarily user safety. Regulatory systems, however, as economists have observed, do not always operate as legislators intend. They are sometimes subject to ‘regulatory capture’ over time resulting in the regulation serving, to some extent, the interests of the industry being regulated rather than the interests of consumers.

Technology-driven business disruption offers new opportunities to reassess regulatory settings across all industries and sectors so that they better serve consumer interests. It should not be assumed out of hand, however, that existing regulation and institutions throughout the economy are necessarily outmoded and obsolete. They have evolved over a long period of time with the intention of limiting risks and protecting both consumers and producers in a way that provides assurances, safety and ongoing trade – that is, enabling markets to function. Generally speaking, it is still too early to tell what should be the regulatory responses to technology driven change, and case-by-case responses will be necessary. But it is clear that governments and regulators need to move quickly and on the basis of sound well-considered principles in order to respond effectively.

A feature of this need to re-consider regulation that is distinctive and relatively new is the need for regulators from disparate parts of the economy, who have hitherto interacted little, to now come together and work more collaboratively on more holistic approaches to regulation. The issues that require regulatory responses are now clearly cutting across different parts of the economy in novel ways: the transport and telecommunications sectors, for example, or finance and communications to cite another. Again, this can, at least in part, be seen as a consequence of the spread of new ICT-based technologies into almost all industries. It is not just that ICT is increasingly present in all industries, it is increasingly becoming of ever greater strategic importance. This is partly due to the ongoing maturation and improving performance of software and computing hardware systems, but is also due to the large advances in reach and ubiquity resulting for the adoption of personal mobile computing devices and the ever more sophisticated apps that run on them.

4.4 The race for scale and the future of market power

One of the early hopes that many associated with the rise of the Internet was for a ‘democratisation’ of marketplaces in which many small-scale sellers could reach many buyers with unique niche preferences. Whilst this has happened, with companies like eBay providing small-scale marketplaces and Google enabling advertisers to operate at any scale, as the Internet matures we are witnessing the rise of globe-spanning technology companies operating international business models that show no signs of reaching a maximum efficient scale. Many of these companies wield significant market power (SMP) and profile themselves as natural monopolies.

This type of development could be viewed as paradoxical: very large companies are enabling markets which enable individuals to trade at a very small scale. But, of course, this is just the development that we should expect from highly saleable, very large information and communications systems with very high storage capacities and very high processing capabilities and with all of these characteristics available at ever falling costs. These new (and not so new) technology companies are using the increasing power and the ubiquity of ICT systems to massively reduce the transactions costs which would otherwise inhibit, or even prohibit, transactions occurring between many individuals.

In one sense, the large ICT companies own the marketplaces they have developed and this ownership will likely confer some degree of market power. It is important, however, not to over generalise or make unsubstantiated assumptions about the nature and extent of this market power, particularly in relation to the formation of new regulatory responses.

These new technology-enabled marketplaces are a substitute (at least in some domains) for traditional marketplaces that have been created through the interaction of business, government and consumers. In many cases - for example, retailing - traditional markets continued to exist and compete with new online markets. Market power will be determined by factors on both the supply and demand side (see below). Further, market power is very much a moving target. The acquisition of market power is a central strategic concern for large firms, and from time to time, their strategies meet with success and failure.

The market power of these technology companies is circumscribed, to some extent, by the potential for further successive waves of disruption, but in the meantime their emergence means the balance of economic and market powers is shifting against traditional players such as telcos, banks, and accommodation and transportation providers. This process immediately raises the question about whether regulation which is being designed to limit the market power that these entities have traditionally enjoyed is now excessive, counter-productive, excessively partial and/or simply unfair.

The rise of the app economy and ubiquity of smart mobile devices seems to create even greater opportunities for companies to offer global scale solutions and systems than does the Internet alone. The outcomes of the interactions between falling transactions costs, falling organisations costs and increasing economies of scale are difficult to predict but some analysts and academics are of the view that these changes will ultimately make technology-driven global corporations more powerful:

*No Coasian analysis of the electronic economy is complete until we assess the impact of distributed information technologies on organizing costs and economies of scale. And in both cases the picture is clear. Simply put, distributed information technologies make it vastly easier to capture economies of scale and coordinate a large firm.*²⁴

²⁴ Phil Agre, The market logic of information, *Knowledge, Technology, and Policy* 13(3), 2000, pages 67-77.

The history of competition regulation in the information technology industry suggests that recurring waves of technological change weaken the market power of dominant firms in the long run. Just as Microsoft unseated IBM in the 1980s, so Microsoft was unseated by the Internet itself and by Google as the 21st Century began. Currently, Google is in ongoing negotiations with EU competition authorities regarding alleged use of its market power in the presentation of search results that favour its own products. The app economy itself provides a challenge to dominant firms in Internet search by providing consumers with alternative pathways to the products and services that they seek²⁵ and social media companies are increasingly competitors in the advertising market. Perhaps again the march of technological change will erode the market power of entrenched dominant firms. On the other hand, the Internet, in combination with the app-economy, offers companies new ways to dominate particular narrow niches:

As diseconomies of scale are destroyed, it becomes more and more practical to run a globally integrated firm -- indeed, a global monopoly -- provided, again, that the firm maintains a strong focus, picking one activity and doing all of it for the whole world. The picture that results is a large collection of focused monopolies, each of them taking a precision "slice" through the world economy by means of global computer networks and by the grace of the standardized world that it both depends upon and helps to create²⁶

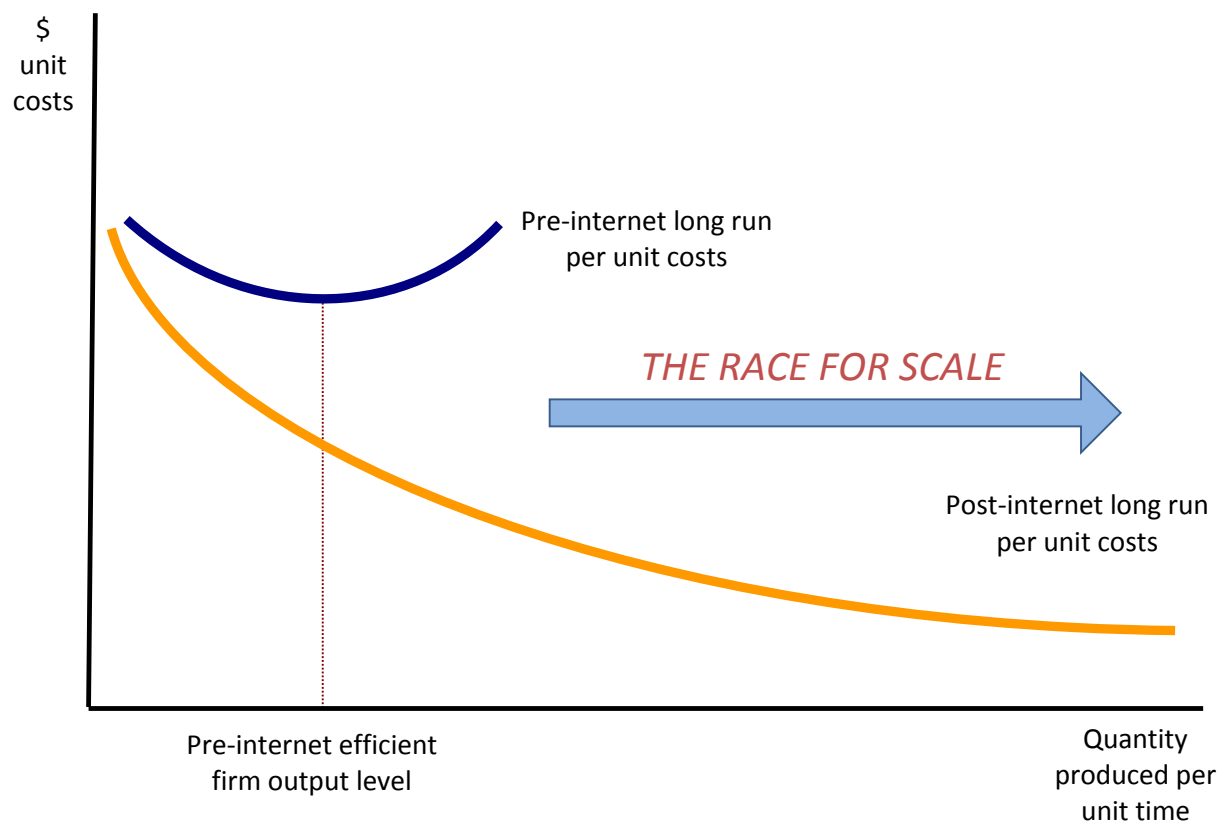
Thus, to continue with the example of Uber, a globe-spanning company has now established a world-wide integrated information system that is challenging all taxi companies in the world by operating a technology solution to the problems of taxi logistics and commerce, while circumventing established businesses. As its scale and level of use increases, its per unit costs fall and it pulls further ahead of competitors because of its lower unit costs.

In this view of the unfolding digital age, the old industrial world diseconomies of scale (represented by the upward sloping section of U-shaped 'Pre-internet long run per unit costs' cost curve in Figure 15) are increasingly artifacts of the traditional world of physical production processes. In the world of physical products, physical stores and physical factories, at some point it becomes an economic grow any larger – stores and factories will become too large to manage effectively and unit costs will rise. As economists put it, eventually there will be 'diseconomies of scale' or 'increasing costs' (meaning increasing per unit costs). This means that at the point unit costs start to rise, the 'maximum efficient scale' of the firm will have been reached. As long as this maximum efficient scale is relatively small compared to the entire market size, there will be room for several or more large firms to compete in the market.

²⁵ www.nytimes.com/2015/08/28/technology/google-eu-competition.html?_r=0 (accessed 27/12/15)

²⁶ Phil Agre, The market logic of information, *Knowledge, Technology, and Policy* 13(3), 2000, pages 67-77.

Figure 15: Decreasing costs and the race for scale



Source: Systems Knowledge Concepts Pty Ltd (www.skcn.net.au)

In the digital world, these traditional long run cost curves are superseded by long run cost curves that continue to slope downwards over any level of production – there are no physical limits to scale; that is, diseconomies of scale never set in. Under such conditions, firms that identify new niches and new business models are in a race at the global scale with the existing or potential competitors. As particular companies such as Uber or Airbnb pull ahead of the competition their unit costs fall and competitors can no longer keep up.

Not only do these economies of scale exist over any level of production, there are positive effects associated with scale on the consumer side as well. Network effects reinforce economies of scale in production. Network effects increase the benefits to consumers from increasing scale of operation and can be encapsulated by the question, why would I join a new social network with hardly any members when almost everyone I know is already a Facebook user? This is the problem that Google faced trying to launch its Google+ social network. Network effects occur because the more users there are, the greater the benefit each user derives. This is amplified by the absence, for the time being, of data portability on social networks, for instance.

In addition to network effects, there are branding benefits that flow from dominance in a particular niche. Facebook is 'the social network'; Uber is ridesharing; Airbnb is online accommodation; and so on. In the many-niched digital world, many consumers tend to associate the single most prominent provider with a particular niche.

Thus, while the emergence of the app economy will likely eventually attract the attention of competition regulators, there are also implications more particularly for sector specific regulators. For example, in relation to telecommunications regulation, the increasing use of apps increases the demand for bandwidth, particularly mobile bandwidth, while at the same time the app economy also tends to weaken the market power of telecommunications companies by commodifying the demand for their services to generic bandwidth at the best possible price. This reduces the capacity of telecommunications companies to market their services and differentiate themselves which will likely lead to lower margins and profitability. The regulatory implications of these changes are discussed in more detail in Section 7.

In terms of international telecommunications/ICT service provision, ITU is working on the identification of relevant markets and significant market power (SMP) addressed to international services and notably multinational companies, in light of the outcomes of the World Telecommunication Standardization Assembly (WTSA-12) and World Conference on International Telecommunications (WCIT-12). An ITU-T Recommendation is under study to propose principles and guidelines to be considered by Member States in defining, identifying and assessing the degree of abuse of market power and dominance by international telecommunication service providers in the various markets for international telecommunication services and obligations on such service providers with SMP²⁷.

Governments and regulators need to find a balance between maximising the benefits of the disruptive app economy while countering the market power of its leading players and balancing sectorial regulation. Increasingly, effective regulation will need to consider its effects across sectors, leading to the need for collaborative regulation between the regulators of various sectors who have traditionally not needed to work together.

²⁷ <http://www.itu.int/en/ITU-T/studygroups/2013-2016/03/Pages/default.aspx>

5 MEASURING THE BROAD ECONOMIC IMPACTS OF THE APP ECONOMY

5.1 What is the significance of the app economy?

As discussed in the previous section, the plummeting costs and increasing performance of converged communications and computing, has led to enormous decreases in transactions costs, as well as a range of other production costs, across all industries. The emergence of the app economy as a new and distinct phase in the development of ICT, more generally, has accelerated this process because of the rapidly expanding reach and availability of mobile smart devices.

Because the app economy appears to be such a powerful phenomenon, it is desirable to establish quantitative measures of its size in order to understand its economic significance. The definition identified in Section 2.2 focuses on the economic activity associated with production of app platforms and apps themselves. It is emphasised again, that, in practical measurement terms, this definition includes unavoidable ambiguities because the app economy is really a subsector of the broader ICT industry.

What do we mean when we are trying to assess the 'size' of the app economy? Typically, what is meant is the dollar value of economic activity. This approach is based on the traditional national accounting methodology which attempts to measure 'value added' for each industry. It is important to emphasise that such estimates on an industry basis have been developed and have evolved over long periods and national statistical organisations have developed sophisticated methodologies based on an array of data sources, including regular surveys.

There are other potential measures of the economic significance of the app economy. These might include: level of employment that it generates, the extent to which it improves productivity in other industries, and the ways that it might contribute to economic growth and development, especially in emerging economies. In this section, potential methods for measuring the app economy are proposed. This is preceded by a discussion of how ICT affects other industries and the issue of ICT and productivity.

5.2 ICT disruption is wide-spread and ongoing: apps accelerate the process

This technology-driven industrial change is unevenly distributed. In some industries, disruption has occurred earlier and has been dramatic than in others. For example, the music industry and newspaper publishing were disrupted early in the cycle and this disruption has been dramatic with only a remnant bricks-and-mortar music retailing surviving and with newspaper publishing seeing ongoing large staff layoffs for well over a decade along with significant changes in ownership. Other industries came later, and can be considered to be in the middle of such a disruption: for example, the taxi industry and the accommodation sector (as already discussed). Today, there is broad recognition that

ICT is impacting all industries and the improving functionality and increasing ubiquity of smart mobile devices is accelerating this effect.

Consider for example the impacts of ICT on:

- **Education** – growth of Massive Open Online Courses (MOOC), and in online-only enrolments (a trend following the previous developments in distance learning models)
- **Retail** – all major retailers now offer online shopping as an alternative to bricks-and-mortar stores and many online only retailers have appeared. Additionally, there is a class of online services that provide price comparison services and offer a range of specials and bargains (for example, Catch of the Day, 1-Day)
- **Banking** – with significant reductions in the use of physical bank branches, cheques, and increasing use of online systems for payment of bills, digital financial services, and all general transactions. An important factor in banking competition is now the quality of their banking apps. Importantly, app-based banking and app-enabled substitutes to money transfers, in the form of trading in mobile minutes has introduced the capability of saving, and micro-transactions are gaining momentum in developing regions. New services have emerged that enable international guest workers to more cheaply repatriate income home.
- **Governments services and systems** – with most aspects of government support and engagement moving to on-line, such as welfare payments, mailing and transport offices (delivering online shopping), and taxation arrangements

While much of this shift was triggered by the internet more generally, the use of mobile devices has seen app-based options evolve and become a part of the landscape: for example, *Blackboard*, the international online education platform used by a large number of universities globally, has now released a mobile version that interacts with the PC-based version. Mobile smart devices make many previously computer-based applications more accessible to more users. For example, users can participate in eBay auctions while undertaking the normal day-to-day activities, instead of needing to be present at a computer when the auction is nearing its endpoint.

The fact that the new generation of smart devices is mobile and personal, coupled with the fact that mobile apps greatly improved access to huge array of commercial services, means not only that very few industries are unaffected by the app revolution, but that very few industries and businesses cannot afford to bring apps and smart devices into their strategic thinking. Because ICT systems generally, and apps specifically, now permeate so many industries and businesses so thoroughly, it becomes increasingly difficult to separate the ICT sector itself from other industries. In a very real sense, ICT and the app economy are interconnecting more deeply industries and businesses across the whole economy. This phenomenon has many implications but, for our purposes, it is important to recognise that this makes the app economy difficult to tightly define and increasingly difficult to quantify meaningfully. In this section we will describe three possible approaches to quantification that consider the app economy from alternative perspectives. This is both a pragmatic approach and recognises that, for the purposes of

policy development, different perspectives will be relevant depending on the types of policies that are under consideration.

5.3 The productivity paradox

It might be expected that these technology-driven disruptions would substantially improve productivity in all of these sectors – but somewhat paradoxically, this period, particularly the last 7 to 10 years, has been one of relatively stagnant productivity growth in developed countries in particular. The economic literature on the drivers of productivity change is large and complex but, generally speaking, productivity becomes increasingly difficult to measure when:

- the rate of emergence of new products is high
- when production techniques are changing quickly
- business models are evolving rapidly
- industrial structures are changing rapidly.

Figure 16: The collaborative economy: participation in the collaborative economy: recent and projected



Source: Sharing is the new buying, www.slideshare.net/jeremiah_owyang/sharingnewbuying

In addition to these factors which impact on traditional measurement methods, some of the apps that are changing industry structures can be considered to benefit final consumers by reducing the final price that is paid for many goods and services, while at the same time having a negative impact on productivity measured by traditional methods. For example, online retailing allows people to find the lowest price for a product, reducing the total value of sales revenue and negatively impacting on traditional productivity measures which are based on market prices. Even further, in the case of retailing, the way in which the internet and apps have facilitated a substantial change in the second-hand goods market (for example, eBay and Gumtree) has further impacted traditional retailing. Again, mobile platforms have made online sales and bidding processes more efficient and widespread – participants no longer need to sit in front of a computer to bid in online auctions.

Thus, the development of the app economy *may be leading to a systematic understatement of national productivity growth as measured by traditional methods and, at the same time, be leading to improvements in consumer welfare that are not being measured*. Such factors mean that measuring and quantifying this recent period of volatile change is challenging for conventional economic methodology. Nonetheless, we want to address questions like ‘what is the size of the app economy’ and ‘what is its economic significance’. Despite the definitional and measurement difficulties, there is a range of approaches that could be employed.

One approach to estimating productivity impacts would be to estimate the impact of technology-driven change on an industry by industry basis. Impacts in some industries have been early and large, while other industries have been left relatively less affected. An important part of such an approach would be to note important differences between different countries and also important differences between advanced, developing and less developed groups of countries. Indeed, some writers have noted how new technologies will enable more rapid economic development in developing countries.²⁸

Such an approach would, in effect, attempt to estimate improvements to productivity on an industry by industry basis while, at the same time, attempting to make allowance for the blurring of industry boundaries that has begun and the emergence of new industries. We note that there are conceptual challenges (as already discussed above) associated with measuring productivity in such a highly dynamic environment and that the data requirements of this approach are quite high, requiring inputs about productivity changes across all industries, or at least those most affected by ICT, in all countries.

An alternative methodological approach would be to examine the emergence of various companies along the value chain, including Apple, Google, Facebook and the more specifically niche disrupters such as Uber, Airbnb, Spotify, Dropbox, SurveyMonkey, etc. In total, the market capitalisation of these and related companies, including those in other countries, such as China’s Alibaba, represents trillions of dollars of value and there is a link between this value and the value created for consumers. This method would

²⁸ *How Developing Nations Can Leapfrog Developed Countries with the Sharing Economy*, Jeremy Rifkin, www.huffingtonpost.com/jeremy-rifkin/developing-nations-sharing-economy_b_8419960.html (accessed 28/02/2016)

enable order-of-magnitude modelling of the economic benefits of the services provided by these businesses. It should be noted that there is not necessarily a tight correspondence between a company's share market value and the utility it creates for users. Some apps are very popular among users and yet they struggle to find a business model that generates sufficient revenue to realise high share market valuations.

The emergence of these services delivered over the Internet and through the mobile telecommunications network, has led to strong growth in consumer demand for fixed and mobile bandwidth. Government policy concerning infrastructure investment, communications regulation and a range of related issues has played critical roles in the development of these services. The price and quality of these services remains a key political issue for many, if not most, governments around the world. The rise of the app economy will likely make the quality and price of these services even more critical, because consumer benefits and economic development will be increasingly linked to these services.

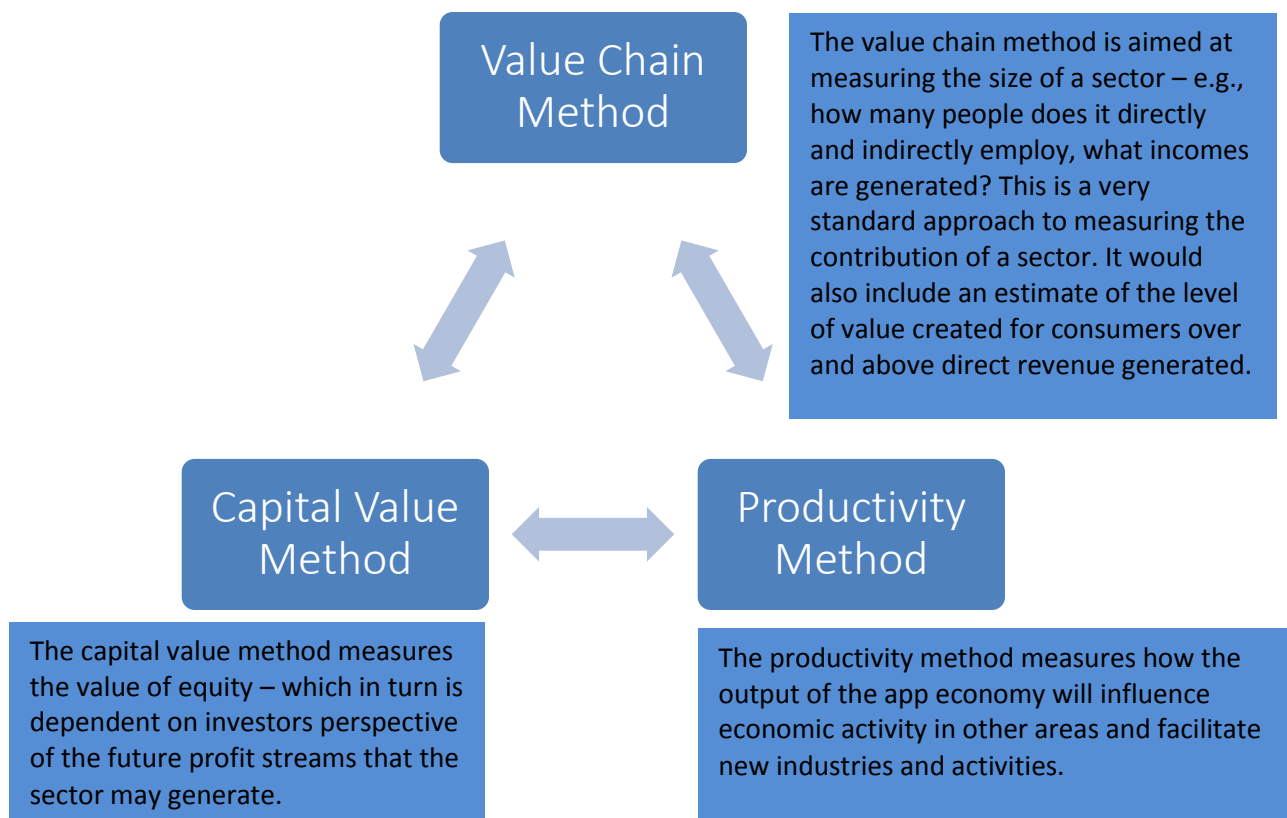
Before governments can introduce policy and regulatory changes, however, it will be necessary to generate more evidence and analysis in support of any changes. It is abundantly clear that the pace of change is challenging the capacity of most governments to respond, and the discussion in this Section identifies some of the challenges for traditional economic measurement and analytical approaches. It should be emphasised that solving these data collection and measurement problems will require significant co-ordinated effort. Traditional data collections will tend to be unhelpful and new sources will need to be investigated and developed. This will take time and, in any case, a better understanding of the economic dynamics will need to be based on longitudinal data, which will need to be collected over a suitable span of time. Below, methods are described which could form a basis for a more comprehensive approach to measuring the app economy and its broader economic impact.

5.4 Challenging traditional industry structures and definitions

One of the characteristics of the app economy is that it disrupts not only traditional businesses and business models, but also traditional definitions of industries. The statistical collections of national statistics agencies are based on conventional industry definitions and are therefore of limited use in describing and measuring the app economy.

Since the statistical data collections that directly measure the value of the app economy are not available, a number of approximation methods will need to be developed and, over time, further refined. Given the multiple ways in which the sector contributes to the economy it is suggested that there are three ways in which the contribution of the sector can be measured. Each measure has different aspects and attempts to value different things, but, taken together, they can be considered as a way to triangulate the contribution the sector makes to the broader economy. These potential measurement methods are illustrated in Figure 17 and each is discussed in more detail below. In addition, a further more speculative method, the value of time method, is also discussed at the end of this section.

Figure 17: App economy measurement methods



Source: Systems Knowledge Concepts Pty Ltd (www.skc.net.au)

5.5 The Value Chain and Consumer Surplus Method

This method is linked to the app economy definition developed above in Section 4.

The level of economic activity in a particular economy is measured by Gross Domestic Product (or GDP) within the National Accounting Framework. The measures are defined as:

- GDP equals Consumption plus Investment plus Government Expenditure plus Exports minus Imports
- GDP is also defined to be equal to Wage and Salary Income plus Gross Operating Surplus

In a global context, exports will equal imports, and so the world GDP is Consumption plus Investment.

Therefore, as a starting point we can measure the economic activity of the apps economy as the value in consumption plus the relevant investment expenditure. Investment expenditure is also a 'predictor' of future consumption, particularly in a start-up technology or industry and can outweigh the consumption value itself. It is important to consider how much development expenditure (i.e. investment) has grown over the last few years as an indicator for where consumption will be in the years to come. The app industry has many aspects of start-ups or entrepreneurial businesses (such as biotechnology) with a long tail of a few large successes offsetting the investment spent on the many that don't succeed. This app development activity is generally funded by a narrow part of the financial market: a combination of personal equity (sometimes funded by mortgages etc. on personal assets), business angels and venture capitalists, governments (funding entrepreneurial activity for economic development purposes), universities, and larger corporations as part of their research and development portfolio. Data concerning all these sources of investment would need to be collected from many sources and it would need to be recognised that even with such a data collection effort, the resulting figures would need to be considered as estimates.

In attempting to estimate the size of consumer value creation, a first step would be to estimate the value of all expenditures by consumers that are required for their participation in the app economy. It is important in this value representation not to double-count, as some products (e.g. handsets) perform multiple functions – for example, a smartphone would be used for simple voice calls on that component of its value to consumers should not be considered part of the app economy benefits. In summary, the relevant costs to the consumer are:

- cost of apps and associated ICT services (this would include direct costs, that is, the price of apps, and indirect costs, such as the implied cost to consumers of having to view advertising in free advertising-supported apps for example).
- The net cost of the 'smart component' of a smartphone for access to these services (conceptually this would be the full cost of a smartphone that allows app access etc. minus the cost of a feature phone with basic telephony access).
- The share of the monthly subscription price that relates to mobile broadband (data) service (versus voice call and SMS access).
- The share of fixed broadband that is available for Wi-Fi access as a basis for mobile app use.

Table 2 summarises the various components of the value chain approach, along with a preliminary perspective of possible sources of data.

Table 2: Components of the value chain

Component of value chain	Sources of data
Global investment and development in app and related start-ups Friends family, business angels Venture Capitalists (VCs) Governments Large corporates Accelerators and incubators Financial institutions	Many sources: investment history of major app companies, industry commentary, summary reports by government or industry representative bodies etc.
App store sales (include Apple share etc.) at national level	Data published by the main app platforms, annual reports, industry commentary and consultants reports.
Handsets - Total value of smartphones sold minus value of feature phone	Annual reports of smartphone manufacturers, industry commentary etc.
Backend – cloud etc. – IT infrastructure	Revenue reports from large-scale cloud providers ²⁹ as well as Industry commentary and consultant reports.
Telecom Operators services –mobile revenue – minus voice and SMS revenues	Annual reports of telcos and industry reports on changes in the composition of revenues to telcos particularly in relation to voice and SMS versus data.
Advertising (not double-counting revenue through Apple and Google)	Commentary and some reports from the mobile advertising industry plus app industry commentary on revenue sources.

Source: Systems Knowledge Concepts (www.skC.net.au)

Once a summary of total consumer expenditure on apps and related services is estimated, consideration needs to be given to the economic concepts of ‘consumer surplus’. Consumer surplus is a central concept in microeconomics and refers to the fact that, in most transactions, consumers receive a benefit from the transaction that is greater than the price they need to pay to secure the good or service. This is depicted in the typical demand curve framework applied in economics (see Figure 18 – total market revenue is showed by the orange rectangle area and consumer surplus by the blue triangle).

²⁹ <http://openviewpartners.com/news/global-cloud-computing-services-market-to-reach-us127-billion-by-2017-according-to-new-report-by-global-industry-analysts-inc/>

Figure 18: The demand curve and consumer surplus

Source: Systems Knowledge Concepts (www.skc.net.au)



This aspect of value creation in the app economy is an important consideration in many areas of new technology. There is a need for primary research in this area, to provide evidence-based quantification of this aspect of consumer benefit. Such research would likely need to include survey work to generate data about consumers' subjective evaluation of apps and app services. There is secondary research available³⁰ regarding consumer surplus values in related markets such as broadband, which could be applied to achieve indicative estimates of consumer surplus values in app markets.

Thus, in order to calculate consumer valuations of benefits related to app services, it is necessary to identify the total amount of consumer expenditure on these services and estimate the average level of consumer surplus. The consumer surplus value is then used to adjust upwards the total expenditure on apps services to arrive at a total benefit figure. It may be worth categorising apps into various types (games, accessing services (transport, banking), online shopping) or into groups of apps with high consumer surplus ratios and ones with lower.

³⁰ Creating new markets : broadband adoption and economic benefits on the Yorke Peninsula / Simon Molloy, Barry Burgan and Sally Rao, Australian Communications and Media Authority, 2008, <http://trove.nla.gov.au/work/34112571?selectedversion=NBD43360631> (accessed 29/02/2016)

For example, assume that, in the app market, for every \$1 million that consumers spend in accessing and using apps, that there is an additional consumer surplus of 50% of the level of consumer expenditure (based on the literature³¹). This inclusion of consumer surplus would increase the value to consumers to \$1.5 million (the original \$1 million of consumer expenditure plus \$0.5 million of consumer surplus). Note that the value of consumer surplus is likely to be different in different countries and for various segments of the app economy. These differences would need to be taken into account in an empirical estimate of the value of consumer benefits.

This type of valuation could be undertaken for a single year and/or calculated for some period of, say, 10 or 20 years using Present Value techniques. The calculation of longer term benefits would require making assumptions about the expected growth rates in the app economy and the use of an appropriate discount rate.

5.6 Capital Value Method

A second measure of value would be to identify the market value of the app providers as an indication of the valuation placed on the businesses that provide these products. The fundamental idea behind this method is that the capital value of companies in a particular sector is related to the value added to the economy by these companies. Having made this point, it is important to emphasise that there are several factors which may cause these valuations to not reflect value-added. These would include: unrealistic expectations about the future value of these companies leading to inflated share prices; monopolistic market structures leading share values to overstate value-added; and sources of value created for society not reflected in share values.

The components of this valuation method would include:

- A proportion of the value of the publicly listed companies that form the core of the app economy (i.e. Apple, Google, Samsung, Sony etc.) and publicly listed companies in other countries. The objective would be to estimate that proportion of each company's valuation that was related to the app economy. This value, for example, would be high in the case of Apple but low in the case of Sony.
- An additional amount for larger corporate private businesses that facilitate the app economy, including the telcos, backbone carriers etc. The proportion of these businesses' activities that were part of the app value chain would be included – for example, data services would be included but not traditional voice services.
- A pro-rata value in smaller and start-up businesses – this would include the entire value of pure app start-up companies and some proportion for those that are only partially app-based.
- Consideration of the fact that some apps benefit users without generating significant capital values for the companies that provide them (often because an appropriate revenue generating model cannot be found).

³¹ *ibid*

An estimate of the total capital value created in the app economy could then be broken down into an annualised value on various assumptions to create an estimate of the annual value generated for consumers (again with assumptions about expected growth rates and an appropriate discount rate).

The table below shows the total market capitalisation of the major contributors in the developed economies, but as noted, the apps-related proportion needs to be extracted by a detailed review of the revenue streams of these entities. This would need to be done across global markets.

Figure 19: Total Market capitalisation of selected key players (in USD billions)

Year	Apple	Google	Microsoft	Amazon	Yahoo	Nokia	Oracle
2005	62.56	61.25	281.66	20.13	56.64	82.29	63.54
2006	70.05	70.42	295.11 ³²	16.60	35.03	83.93	88.62
2007	174.96	108.06	337.92	37.89	31.34	151.89	117.99
2008	76.83	48.37	171.51	21.77	16.61	59.94	89.97
2009	189.50	98.41	273.65	60.36	23.71 ³³	47.71	125.33
2010	299.77	95.33	239.64	81.28	21.42	38.12	159.50
2011	378.59	104.50	219.05	80.16 ³⁴	19.96	17.73	128.79 ³⁵
2012	582.57	116.60	226.07	112.62	23.15	15.03	159.12
2013	501.31 ³⁶	188.00	312.55	185.10	41.24	29.55	169.13
2014	668.53	361.44	394.67	143.11	48.14	30.05	202.44
2015	598.34 ³⁷	515.76 ³⁸	437.82	311.96	31.13	26.08	155.47

NB. Nokia is now been acquired by Microsoft.

Source: Various – see footnotes

5.7 Productivity Method

This method would probably be the most difficult to execute because of a lack of data, despite a significant base in the economic literature on the importance of productivity growth as the core source of per capita increases in income over time³⁹. The fundamental

³² Dip between 2005-6 down to 225 billion

³³ Peak between 2008-9 up to 39 billion

³⁴ Peak between 2010-2011 up to 110 billion

³⁵ Peak between 2010-11 up to 182 billion

³⁶ Peak between 2012-2013 up to 657 billion

³⁷ Peak between 2014-2015 up to 750 billion

³⁸ 23/12/15 – *Ycharts*

³⁹ Jalava, J, Pohjola, M, Economic growth in the New Economy: evidence from advanced economies, Information Economics and Policy, Volume 14, Issue 2, June 2002, Pages 189–210

Edwards, S., 1998. Openness, productivity and growth: what do we really know?. The Economic Journal, 108(447), pp.383-398.

Fischer, S., 1993. The role of macroeconomic factors in growth. Journal of Monetary Economics, 32(3), pp.485-512.

concept is to investigate the extent of digital disruption on a sector by sector basis and estimate the increases in productivity caused.

Given that the level of economic activity in each sector is well known given national accounting data collections, it would therefore be possible to attribute a boost to national economic activity arising from the disruptive effects of the app economy.

This method would also involve some novel thinking about the nature of productivity change and would require some speculative 'what if' type economic modelling which would entail making various assumptions about the relevant productivity changes and factoring these into various modelling scenarios. This would enable testing the sensitivity of the conclusions to these various assumptions. This type of approach would be required because, as we have noted above, traditional productivity measures are of limited use when evaluating such a dynamic influence on economic activity as the app economy.

The steps required to model the value using this approach would be:

- To categorise the world economy into country (or country group – such as developed economies, developing economies etc.) and industry groups (IT sector, manufacturing, services etc.). The objective of this categorisation would be to identify industries according to the extent of impact of the app economy. The classification of economic activity that resulted from this step in the process would likely be different from traditional industrial classifications.
- For each of the industry groups, using information from industry studies with respect to how digital disruption and use of apps is impacting on the industry, and from various case studies develop a scenario of the extent to which productivity has improved due to the app economy within each country or country group. In essence, this would be a pragmatic exercise that entailed examining those industries which appear to be most impacted by the app economy and developing estimates of the productivity impacts. These estimates would then be used in the 'what if' analysis described above.
- Model the whole of economy impacts of these scenarios of productivity change based on assumptions of elasticity of demand and supply for these industries. Elasticities of supply and demand have significant effects on how changes in cost structures and productivity translate into profits for business and benefits for consumers. In effect, these elasticities determine how the gains from productivity are shared between these two groups.

The core outputs of this modelling would be the increase in real incomes (per capita) as a consequence of the growth of the app economy.

5.8 Value of time method

This method is somewhat more speculative, but at the same time potentially more expedient than the other methods discussed. Many goods and services can only be consumed if the consumer is willing to spend time consuming them. Movies, books and many other entertainment products are good examples. Similarly, apps and

communication products are typically associated with specific dedicated allocations of time in their consumption.

The economic basis of this proposed valuation method is that consumers value their own time and that if they are willing to dedicate time to consuming 'time intensive' goods and services then the value of time that they are willing to sacrifice consuming these goods represents a lower bound to the value that they place on them.

This measure is potentially interesting in the context of the app economy because telcos and app companies generally have good data regarding the amount of time users spend using telecommunications services and apps. Actually putting a value on time is somewhat complex: allowances would need to be made regarding variations in the opportunity cost of time in different jurisdictions, considerations regarding whether consumers regarded themselves as in 'recreation or work mode' and various other technical considerations regarding the value of time. Notwithstanding these specific data challenges, if aggregate measures of consumers' allocation of time to apps and telecommunications services could be identified, then these could be used as a basis for estimation of the value of the app economy to consumers.

5.9 Commentary on potential measurement methodologies

The objective of this section of the report was to generate a set of prospective methodologies for measuring the value and economic contribution of the digital platforms and app economy. The methodologies discussed in this section are based on traditional economic methodologies applied to new types of data being generated by the growth of the app economy. As has been emphasised previously, the disruptive nature of the app economy growth means that traditional data sets corresponding to existing industry structures are of little use.⁴⁰

The size of the task associated with constructing meaningful, robust and defensible estimates of the size of the app economy should not be understated. Drawing together data sets from multiple countries from relatively new and potentially incompatible sources over multiple years is a very large task. Moreover, the target is moving rapidly; some countries are already collecting some data through their National Statistical Office. However, discussion is required at the international level on the optimal approaches to measuring the app economy. Early consensus on this issue would allow the collection of consistent data to commence.

⁴⁰ It should be noted that the current system of *System of National Accounts* ('SNA') (available at <http://unstats.un.org/unsd/nationalaccount/sna.asp>) is the internationally agreed standard set of recommendations on how to compile measures of economic activity dates from 2008. While the related documents such as the International Monetary Fund (IMF)'s *Balance of Payments and International Investment Position Manual* was updated in 2012 (BPM6), it is likely that globally further revisions and adjustments will be required to the SNA (and subsequently how it is applied by national statistical bodies) so as to reflect the development of the app economy, economy wide transformation and to better capture national economy activity sooner rather than later.

6 REGULATING THE APP ECONOMY

6.1 Introduction

The app economy is going mainstream,⁴¹ it is challenging businesses across multiple industries and this has inevitably led to significant debate about what forms of regulation, if any, are optimal. This debate is observed most publicly in legal disputes in a range of markets concerning *inter alia* both ICT sector ‘disruptive’ entities such as Netflix, Google, Apple, Facebook/WhatsApp, Tencent/Wechat, LINE and Viber, and Uber and Airbnb.

There are a number of factors that drive the uptake of ICTs. One factor that has been identified as key in this process is the regulatory environment. The right regulatory environment can ensure that consumers can use the full palette of new opportunities and services made available by the greater choice of devices, online services and applications. The regulatory environment needs to find the best possible trade-offs between consumer protection, investment and innovation for the whole of society. Regulators around the world have endorsed a set of best practice guidelines to protect consumer interests while ensuring a level-playing field for traditional and new market players by fostering a light-touch regulatory approach (see Figure 20 below).

OECD also recognized the importance of the app economy in a 2012 report (DSTI/ICCP/IE(2012)1/FINAL) and provided that:

Apps are one of the main new sources of innovation in the economy and remain an area of spectacular growth during this economic downturn. Mobile apps enable significant efficiency gains by improving the way people communicate, access information and obtain services. Apps extend the rich communication potential of the Internet beyond the traditional desktop computer and enable users to benefit from a myriad of information services practically anywhere or anytime they want. Economies rely on information to function effectively and the app economy represents a leap forward towards the goal of an informed and efficient knowledge-based society.

The app economy is extremely dynamic and evolving, and policy makers are keen to maximise its innovative potential and benefit for all sectors of the economy and society. Policy makers need to understand the mechanisms of the app economy in order to support innovation and ensure the maximum benefits possible for users.

The app economy is inherently global and this, in itself, has an impact on regulation. Ideally, a unified global approach to regulation is desirable but is unlikely to be operative in the short, or even medium, term. Regulation does not occur in a vacuum, and the establishment of a legal and regulatory framework is determined in large part by each country’s specific legal tradition, today regulators and industry players are struggling with this issue.

⁴¹ See Richard Waters, *Sharing economy starts to go mainstream*, Financial Times, 2 July 2015

Figure 20: ITU GSR Best Practice Guidelines

For over fifteen years, the ITU Global Symposium of Regulators (GSR) has brought together heads of national telecommunication/ICT regulatory authorities from around the world and has earned a reputation as the global annual venue for regulators to share their views and experiences. Every year, GSR adopts Best Practice Guidelines on topical regulatory and policy issues.

In 2015, GSR adopted Best Practice Guidelines to facilitate the widespread adoption and use of mobile applications and services through targeted regulation. The 2015 Best practice Guidelines also urged regulators to simulate demand and protect consumers and suppliers, Regulators recognized the importance of facilitating availability, access and use of m-services and digital apps by stating:

“New generation networks are the foundation of innovation in the ICT sector and the engine for the development of m-services and applications. Therefore, we believe that unified rules for facilitating infrastructure deployment and open access to networks at national and regional level can strongly contribute towards stimulating the development of m-services and apps. Cooperation among all public authorities involved at the international, regional, national, and local levels is key to rapid, smooth and efficient implementation. Policy makers and regulators must be mindful of 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, so as to create trust and provide the necessary conditions for m-services and apps markets to thrive. The development of new markets and the industry for mobile devices need to be sustained through adequate regulatory measures, in particular in developing countries.

Revisiting and reviewing, where necessary, current Government policies to make sure that they are still valid and appropriate for the new environment and ensuring privacy and security of government, business and consumer data may be necessary while open and collaborative regulatory frameworks are needed to promote the development of cross-cutting services such as m-commerce, m-banking and mobile money, as well as m-health. We recognize that creating a converged reference framework for competition, interconnection and interoperability can effectively facilitate the relationships among the various providers of infrastructure and services, as well as among them and apps and content providers.

Recognizing that it may be commercially attractive to share network elements between service providers to avoid duplication costs, and provide opportunities for more m-services to be made available, regulators may consider promoting network sharing practices in all network and value chain layers while maintaining healthy competition between network providers. We believe that innovative, out-of-the-box measures should be put in place to stimulate the take-up of m-services and the creation of locally-relevant apps in remote and rural areas.

Among other measures, universal service strategies can be defined and the appropriate mechanisms used to create ICT incubators or for funding local developers and locally-relevant apps. We call for regulatory measures, private initiatives and partnerships to reduce the cost of m-services and apps in order to ensure equal and universal access. We further recognize that acquiring digital skills is essential for the wide take-up and efficient use of m-services and apps, and inclusive training programmes for different target groups need to be established. We reiterate the relevance and value of the GSR13 Best practice guidelines on the evolving roles of both regulation and the regulators in a digital environment; and of the GSR14 Best practice guidelines on consumer protection in a digital world.”

Source: GSR-2015 Best practice guidelines⁴²

⁴² www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Consultation/BPG_2015_E.pdf

In 2015, the European Commission launched its much-trailed Consultation on Online Platforms, Cloud and Data, Liability of Intermediaries, and the Collaborative Economy⁴³. The Consultation is part of the Commission's assessment of the role of online platforms, promised in its Communications on a Digital Single Market Strategy for Europe on 6 May 2015. The enquiry asks whether platforms should be left to market dynamics, self-regulated or subject to regulatory measures

The Commission has summarised the scope of the Consultation as:

the social and economic role of online platforms, transparency (e.g. in search results), terms of use, ratings and reviews, the use of information by platforms, the relation between platforms and their suppliers, the conditions of switching between comparable services offered by platforms, and the role of online intermediaries, including ways to tackle illegal content on the Internet.

The latter has already generated a substantial level of commentary and debate within Europe and no doubt this is but the start of a broader dialogue in that market and globally. Industry stakeholders are concerned that the review will lead to developing unnecessary regulations for the Internet economy. This debate will undoubtedly play out in 2016 and beyond.

Irrespective of the approach, top-down, or industry by industry or by the courts the fact is, for the app economy to thrive, legal provisions are needed, and at the same time the applicable body of law must not hamper the spread of innovation and progress within the app economy. This is indeed a balancing act especially since most regulation is national (or in the case of Europe regional) when the app economy is in many ways 'born global'.

6.2 Preconditions for the development of platforms

Although the business models themselves may differ greatly from one sharing economy market to another, successful peer-to-peer platforms typically have three core attributes, which need to be acknowledged in any approach to regulation of the app economy.

First, the platform must create opportunities for sellers and buyers to do business with one another. This means attracting potential sellers and buyers to become users of the platform.

Secondly, peer-to-peer platforms need to be able to assist buyers and sellers in reaching an agreement. They need to have a way of determining or negotiating a price and other relevant terms of the transaction.⁴⁴

Third, peer-to-peer platforms need to ensure that buyers and sellers can conclude their transaction in a mutually satisfactory manner. In other words, there need to be mechanisms for creating trust between the parties and for addressing problems that may

⁴³ <https://ec.europa.eu/digital-single-market/en/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud>

⁴⁴ Interestingly when Airbnb first started it identified an interest in renting rooms and spaces but individuals had no clear way to price such services. So Airbnb created an algorithm to provide a guide to their hosts.

arise. Almost all platforms have adopted reputational rating mechanisms (first popularised by ebay) in order to provide a crowd sourced view of the reputation of the seller/host/driver/supplier etc. The latter is important as there is a high degree of self-regulation in the app economy which can mean that there can be less oversight by regulators (at least conceptually).

6.3 Addressing Government, regulator and key stakeholders

In formulating the optimal approach for the regulation of the app economy there is a need to address Governments, regulators including both ICT and non-ICT regulators, and key stakeholders. Suggested generic advice to businesses in addressing sector regulators is set out in Figure 21.

Figure 21: Suggested advice to businesses in addressing sector regulators and stakeholders

Be collaborative (rather than defensive) with regulators: The app economy is a new concept and as new business models are involved these may be unfamiliar to existing market players including regulators. Increasing understanding takes time. There is often an assumption that sharing economy firms are trying to make a profit by skirting the regulations 'traditional' industries face. Without explaining the nature of your firm clearly to regulators you will likely be regulated as a traditional market player not as say, an intermediary (providing a platform for consumers rather than providing services directly) resulting in higher taxes and requirements.

Be responsive to regulators' legitimate concerns: Many app economy business models do raise legitimate concerns about user safety, privacy and access. These need to be addressed such that entities proposing new models should make compelling arguments they would believe if they were regulators.

Use state of the art approaches to reaching out to government: The best practices in approaching government include, forming coalitions and industry associations to represent a shared point of view rather than each company approaching regulators independently and only in times of crisis. There is a need to be an active participant, taking part in open consultations, seeking place on the decision-making table, being open and transparent about one's expectations and the challenges ahead. Further, app economy firms should seek outside validation from external third party stakeholders.

Share your data: Data need not be made public in order to share it with Government, and can help your case by reducing regulator concerns.

Make a well-researched case for the value provided by your firm: Rather than relying on maxims about the usefulness of the app economy, it helps to have concrete data.

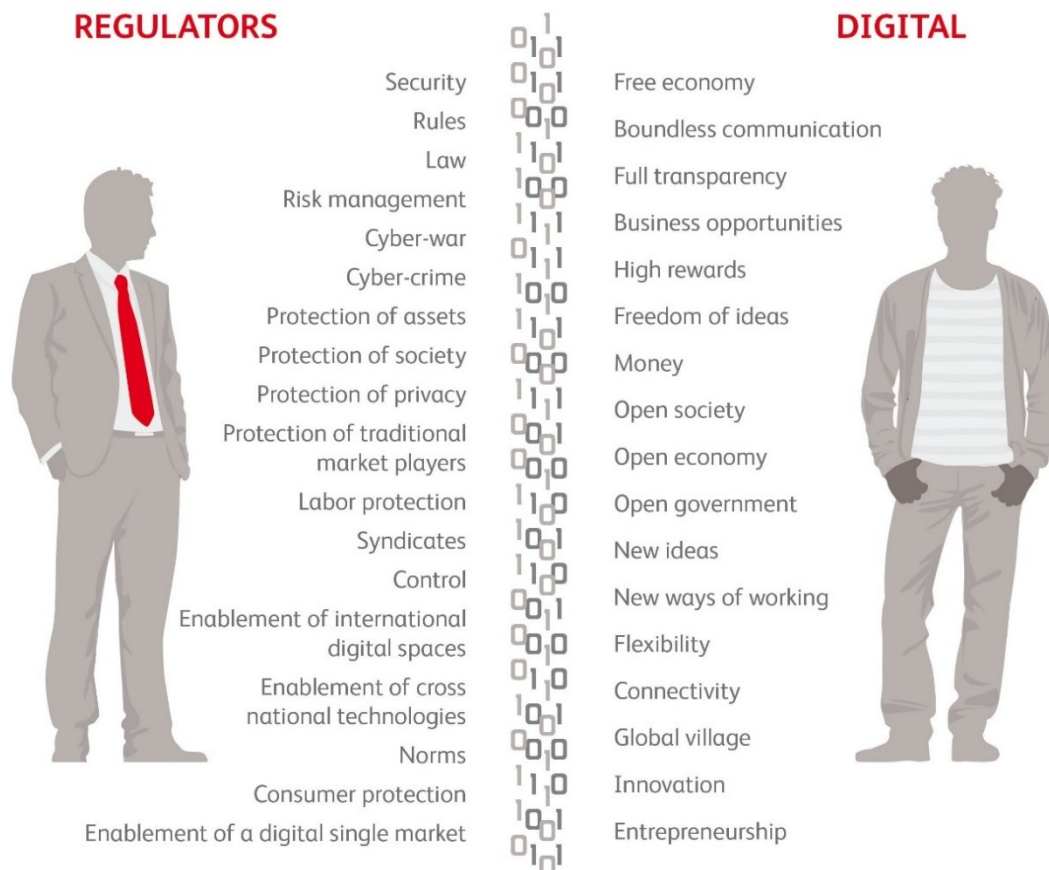
Find the best regulations out there and share them with the Government: Governments are often under-resourced and many existing rules are simply out-dated and are not relevant given the business model of app economy firms. There's no reason firms themselves cannot find the best rules out there and propose such optimal rules. Having said that, industry has specific (and often technical) knowledge and experience of business that they could contribute to the discussion – in order to avoid decisions and regulation not solidly grounded.

Source: ITU modified version of Sarah Cannon and Lawrence H Summers, How Uber and the Sharing Economy can win over regulators, Harvard Business Review, 13 October 2014.

6.4 The debate on optimal regulatory approaches

As part of the debate on optimal regulatory approaches, some have called for the **creation of a digital services category** with the reclassification of traditional communication services, followed by the reorganisation of the associated obligations such as transparency and non-discrimination, security, privacy, data retention, emergency services, interoperability and portability.

Figure 22: Different perspectives on the app economy and its regulation



Source: Bearing Point, 2015. NB, Digital refers to digital sector market players.

In the United States, Chairwoman Edith Ramirez of the US Federal Trade Commission (FTC) in October 2015 discussed the growth of the sharing economy for regulations that preserve competition and customer protection.⁴⁵ She indicated that central to this discussion was the question of how to balance regulations for established businesses and newer, innovative businesses. While the former often has strong consumer protections built up over years, the latter benefits from avoiding these regulations. At the same time, innovation could be hampered by regulations tailored to a specific (arguably legacy)

⁴⁵ Keynote Remarks of FTC Chairwoman Edith Ramirez 42nd Annual Conference on International Antitrust Law and Policy Fordham Law School New York, 2 October 2015. Available at www.ftc.gov/system/files/documents/public_statements/810851/151002fordhamremarks.pdf

business model. Capturing the benefits of innovative business models will require regulations that allow for growth without sacrificing consumer protections developed over many years.

Chairwoman Ramirez indicated that the FTC had “cautioned state and local governments not to impose legacy regulations on new business models simply because they happen to fall outside of existing regulatory schemes. The threshold question for policymakers examining new peer-to-peer businesses should be whether there is a public policy justification for regulating the service at all, either through an expansion of existing regulatory schemes or entirely new ones. If there is no public policy rationale justifying regulation, policymakers should allow competition to proceed unfettered.”⁴⁶ It was the FTC’s view that in their experience consumers generally benefit from the competition that arises between traditional and new business models.

Chairwoman Ramirez strongly advocated against the establishment of a ‘two-track’ regulatory regime for old and new business models. Regulating established businesses differently from newcomers would confer an unfair advantage to whichever model had the least costly regulations. Established business models should not be punished for complying with regulations, nor should new businesses be punished for innovating. Harmonizing regulations between new and old industries would preserve consumer protections without hindering innovation. There is no need to reinvent the wheel for sharing economy regulations when a mere extension of existing consumer protections may be all that is necessary. This is of course, easier to say than for Governments to do.

Other industry stakeholders hold even stronger positions as summarised in Figure 23 below

Figure 23: The case of less rather than more regulation for the sharing economy

Globally a range of organisations are arguing the case for less rather than more regulation for the sharing economy. In Europe, in response, with respect to EU collaborative economy consultations which will run through to early 2016, the Technology Policy Institute advises policy makers to dismantle policies that primarily protect incumbent operators. Policy makers should also resist applying the rules regulating incumbents to new market entrants; instead the appropriate response should generally be to lower the requirements for incumbents.⁴⁷

In Australia, the Institute for Public Affairs similarly recommends that liberal regulatory approaches be instituted to promote the growth of the sharing economy, including:

- The encouragement of bottom-up, self-regulating institutions prior to introducing top-down government controls;
- The reduction of occupational licensing, to allow private certification schemes and reputation mechanisms to evolve;

⁴⁶ *ibid*, page 7

⁴⁷ Refer to https://techpolicyinstitute.org/press_release/ec-proposals-may-impact-entire-internet-economy/

- Industry specific regulatory frameworks need to be avoided;
- Regulations making it harder for start-ups to compete for labour need to be reduced; and
- The status of individual contractors needs to remain separate from highly restrictive employment law.

Source: Darcy Allen and Chris Berg, The sharing economy How over-regulation could destroy an economic revolution, IPA, December 2014

An example of ‘light touch’ regulation is Singapore’s *Third Party Taxi Booking Service Providers Act 2015* summarised in Figure 24.

Figure 24: Singapore’s Third-Party Taxi Booking Service Providers Act 2015

Recent innovation in the shared economy has caused disruptions to the transportation sector. In response, the Singapore Government has chosen to regulate all third-party taxi booking services.

The *Third-Party Taxi Booking Service Providers Act* takes a ‘light-touch’ approach to regulation by only imposing basic requirements that are necessary to protect commuter interests and the ‘fundamental tenets’ of taxi regulatory policies. Under the regime, all third-party taxi booking services with more than 20 participating taxis are required to register with the Land Transport Authority (LTA). The threshold of 20 is to allow very nascent services to be exempted from registration, providing them room to ‘experiment’ before their size reaches the registration threshold. Furthermore, clause 11 of the Act empowers the LTA to impose conditions on registered providers to ensure that commuter interests are safeguarded and taxi regulations are not undermined. These conditions include the requirement that registered service providers must dispatch only licensed taxis and drivers holding valid Taxi Driver’s Vocational Licences, fare-related safeguards for commuters and the existence of customer support services for commuters.⁴⁸

Upon an overview of the Singaporean legislation, it is obvious that the ministry intended not only to minimise disruption and protect consumer interests, but also to allow space for new services to innovate and thrive, and for new technologies and business models in the market to emerge.⁴⁹

In summary, while there are many approaches which may be adopted, there is no compelling case for one to be recommended. It is simply too early to say, as the app economy has not been around for long enough nor are there examples of significant market failure which warrant prescriptive rule making. What is clear, however, is that (i) new models for the app economy are important, collaborative regulation has merit and is being embraced by users and (ii) that light-touch regulation, if any, ought to be preferred.

Over time a single regulatory treatment (as opposed to the two-track approach) of sectors, market substitutes, competitors etc. will become necessary as what was new and innovative becomes the norm. In the telecommunications/ICT sector in order to preserve *inter alia* competition and a level-playing field, this may necessitate reduced regulation, less operator obligations and more transparency with respect to sector cross-subsidisation.

⁴⁸ www.mot.gov.sg/News-Centre/News/2015/Second-Reading-for-Third-Party-Taxi-Booking-Service-Providers-Bill-by-Minister-for-Transport,-Lui-Tuck-Yew,-in-Parliament-on-11-May-2015/

⁴⁹ www.lta.gov.sg/apps/news/page.aspx?c=2&id=193b3496-9acd-4473-833e-b2b5d2bf5eaa

6.5 Exploring key regulatory questions for the ICT sector

6.5.1 Overview

Currently, collaborative economy platforms often exist in regulatory grey areas. That is 'sharing economy' platforms, often operate outside the scope of the specific national regulations that apply to their industry, current competitors and may in fact be incompatible with traditional forms of regulation.⁵⁰

Such is the speed of the broadband and smartphone revolution that collaborative business models were not anticipated by regulators, and therefore there were no rules drafted to govern these entities. It is not all too surprising, that Government policy can struggle to keep up with technological innovation and corresponding move away from traditional approaches. This has happened before in the ICT industry with the explosion of mobile services and is likely to happen again in the future given rapid technology innovation.⁵¹

However, collaborative platforms in the app economy do not exist yet in a legal vacuum. The best example of the application of rules, even though it is outside the ICT/Telecommunications sector is case of Uber (see Figure 22 below).

Figure 25: Uber, a case where the primacy of service is overcoming regulatory uncertainty

Uber's recent expansion demonstrates the ability of a sharing-economy platform to overcome regulatory uncertainty to provide services whilst fostering new competition in existing markets.

The legality of the ride-sharing app Uber has been a topic of great contention since the platform's inception in 2011. Uber Technologies Inc. is involved in numerous lawsuits internationally, amidst protest from taxi industries and governments. However, the growing primacy of the platform in regions with well-established taxi industries has shown that there is great market demand for the app..

Non-ICT Regulators and legislators globally have taken divergent approaches to the Uber platform. Uber has been the subject of claims that their drivers are not licensed to drive taxicabs, and hence that the application operates illegally. In Spain, France, and Thailand, the service has been banned outright.⁵²

⁵⁰ For example, there have developed over time very comprehensive classification systems for audio-visual content many of which are national and tailored for national cultural and religious norms and traditions. However, global web content including streaming of audio-visual content, often does not adjust the delivery based on geographical location and/or such classification systems. While globally games typically use the PEGI classification system – see www.pegi.info/en/index/ this is not the case for other content resulting in actions like Indonesia's largest operator Telkom Indonesia currently blocking Netflix's content in Indonesia.

⁵¹ While perhaps now forgotten there was a considerable debate about how cellular mobile services should be regulated and whether fixed line regulatory models should apply to wireless technologies. Likewise about VOIP. So in a way, the debate about the optimal regulatory regimes for OTT and similar services is nothing new.

⁵² www.businessinsider.com/heres-everywhere-uber-is-banned-around-the-world-2015-4?IR=T

However these countries form a small exception to the now-large range of markets where Uber is in successful and authorised operation.⁵³

Furthermore, the benefits of the platform are increasingly being recognized. Uber gives consumers a choice between regulated taxi companies in their area, and other forms of transport. Users can track their driver on approach, their own journey, and pay over the internet with their smartphone.

More broadly, the app creates jobs for drivers, together with competition for often- inefficient and ineffective taxi industries. Uber is increasingly being recognized as a superior service to traditional taxis. Reviews of the platform cite Uber as favorable in terms of price, reliability, and overall experience.⁵⁴ Therefore, Uber represents how collaborative business models can overcome regulatory uncertainty to provide new services and competition within existing markets.

Source: Author analysis of industry sources

More broadly, a continuing policy issue relating to the app economy is the need to provide users with meaningful information and control over how platforms are using personal data.⁵⁵ The debate about the use of personal data is a significant issue in and of itself and has been the focus of separate regulatory reviews in a range of markets in Europe, the Americas, Asia and elsewhere.⁵⁶ Data protection and privacy is also a topic which will be explored at the ITU GSR16.⁵⁷

Most significantly, a key risk to sharing platforms is government policy, in many cases driven by current industry incumbents. Regulators must find the balance between consumer concerns, and claims by existing incumbents that seek to protect their own market position or the primacy of their businesses.

It remains necessary for regulators to adapt and clarify existing regulatory schema to account for collaborative and app economy platforms. Doing so would provide all operators, businesses and consumers with greater legal certainty. Regulators – both in the ICT sector and beyond must therefore negotiate the difficult line and find the appropriate balance between ensuring consumer security, product quality and other protections in transactions; while at the same time creating the enabling environment for investment and innovation and avoiding over-regulating new business models.

Rather than simple two-sided marketplaces that match people looking for a service with others willing to supply it, over time it is expected that the business case will create the framework where there will be a greater responsibility for the delivery of services, meaning that business cases will consider engaging more at local level and consider greater local human and financial resources including hiring workers locally, and

⁵³ www.uber.com/cities

⁵⁴ www.choice.com.au/transport/cars/general/articles/uberx-vs-taxi-which-one-is-best

⁵⁵ [www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/IE\(2012\)1/FINAL&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/IE(2012)1/FINAL&docLanguage=En)

⁵⁶ Data privacy legislation or revised data privacy legislation has now been enacted in a majority of global markets. By January 2015 the total number of countries with data privacy laws totalled 109 and such legislation is expected to become ubiquitous. See detailed discussion in Graham Greenleaf, *Global data privacy laws 2015: 109 countries, with European laws now a minority*, (2015) 133 Privacy Laws & Business International Report, February 2015 UNSW Law Research Paper No. 2015-21 . Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2603529

⁵⁷ www.itu.int/en/ITU-D/Conferences/GSR/Pages/GSR2016/default.aspx

channelling back financing assets to the local economies in the process. Developments such as these may leave sharing economy companies, for better or worse, looking far more like other types of business. This is the process of integration of online services into the general economy and broader economic activity. Online services instead of being ancillary, an adjunct business channel or similar becomes fully integrated within business models, delivery platforms and central to business activity.

6.5.2 Taxation issues

While beyond the scope of this report, taxation and related regulations will also need significant updating in order that there is not a significant erosion of the tax base. It is important to note that this has already been the subject of considerable debate in a number of countries and in international institutions such as the Organisation for Economic Co-operation and Development ('OECD')⁵⁸ and others.

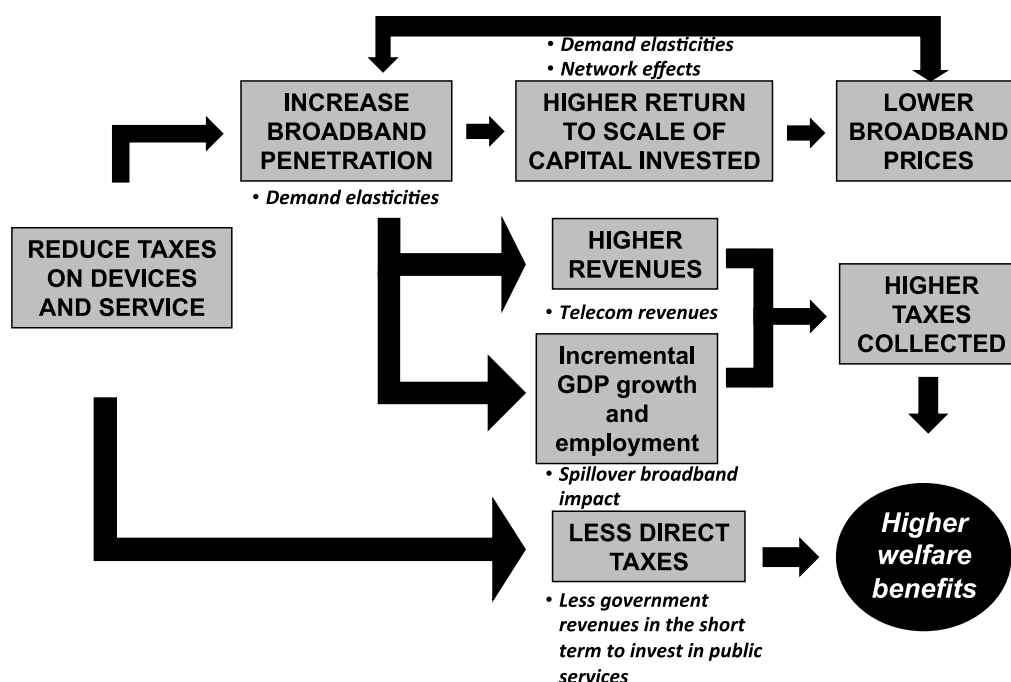
In a recent ITU study, *The Impact of taxation on the Digital Economy*⁵⁹, policy issues related to the taxation of firms operating within the digital sector are discussed, as well as levies imposed on consumers purchasing digital goods and services. As indicated in the title, its scope is wider than just telecommunication services, although it also addresses taxation of telecommunication/ICT operators.

This study explains that at the highest level, two opposing trends can be defined in terms of digital taxation policy: one aims to maximize collections based on exponentially growing digital flows; the second one recognizes that lowering taxation benefits consumers and businesses, and consequently, economic growth. According to the first trend, governments recognize that digitization is critical in their generation of revenues and are putting in place more mechanisms to maximize collection in these domains of economic activity. On the other hand, some countries consider that lowering taxes on the digital sector of the economy triggers spillovers that are larger than the foregone taxes. This effect in the case of broadband taxes is depicted in the Figure 26 which shows the Virtuous Circle of Tax Reduction on Broadband Devices, Equipment and Services.

⁵⁸ See recent report, *Addressing the Tax Challenges of the Digital Economy*. Available at www.oecd-ilibrary.org/taxation/addressing-the-tax-challenges-of-the-digital-economy_9789264218789-en

⁵⁹ www.itu.int/pub/D-PREF-EF/en

Figure 26: Virtuous Circle of Tax Reduction on Broadband Devices, Equipment and Services



Source: Katz, R. and Berry, T. (2014) Driving Demand of Broadband Networks and Services. ITU Publication “The Impact of taxation on the Digital Economy”.

Figure 27 also highlights Australia’s Netflix Tax while Appendix A to this report provides details of the OECD Base Erosion and Profit Sharing (‘BEPS’) reforms and specific implications for OTT players.

Figure 27: Australia’s ‘Netflix Tax’ and Similar Global Regimes.

In response to the OECD report and soon after Netflix’s introduction into Australia at the beginning of 2015, the Australian Federal Government proposed to amend the Goods and Services Tax (GST) law to ensure digital products and services receive an equivalent tax of 10 percent, whether they are provided by Australian or foreign entities. Consequently, digital products and services such as Netflix will be taxed from 1 July 2017.⁶⁰

This approach of the Australian Government is an attempt to level the playing field for domestic businesses in Australia and to close a ‘digital tax loophole’. Under the current law, digital products and services such as Netflix are not subject to the GST, yet the same digital products and services provided by domestic businesses are. This results in forgone GST revenue to the States and Territories and places domestic businesses at a tax disadvantage when compared to overseas businesses. The scheme will cost the Australia

⁶⁰ www.gizmodo.com.au/2015/05/the-netflix-tax-everything-you-need-to-know/

Tax Office (ATO) AUD1.5 million to establish, and is forecast to raise AUD150 million from Australian consumers in its first year of operation and AUD200 million in its second year.⁶¹

Similar taxation laws aimed at targeting the digital economy have been introduced in the European Union (EU). At the start of 2015, the EU begun to overhaul its consumption tax (value added tax or VAT) to extend it to providers of broadcasting and electronic services based on the location of their customers, instead of where the companies set up their head offices. Digital downloads and services sold to European retail consumers are taxed VAT rates of up to 27 percent, making the digital retail economy a significant source of tax revenue.⁶² The complexity and variation of VAT regimes in different EU member countries, however, has created huge challenges for the EU and the digital companies.

The United States has also attempted to pass an Internet sales tax that would force online retailers such as Netflix to collect sales taxes for state and local governments, even if the companies do not have a physical presence in the state. However, US Congress has yet to pass such a Bill.⁶³

6.5.3 Specific approaches to new ICT market players

It is also critical to explore key ICT regulatory questions as the regulation applying to such services (including OTT services) has a material impact not only on the telecommunications and IT sectors but on the uptake of such services in all other sectors of the economy. The ability and flexibility to embrace technology diffusion has a profound effect on a country's ability to take advantage of the transition to the app economy and increased consumer surplus arising from innovation and disruption.

As noted by an industry commentator on developments in the technology sector at the 2016 World Economic Forum in Davos: *"Why is innovation so important? In the technology driven world that we live in today, we see the digital influx in every sphere of our lives – whether it is in our workplace, our homes, our cars, our lifestyle and even our health. Going forward, the impact which technology and innovation will have upon our lives is likely to increase, and not decrease. It is therefore not surprising that many more governments around the world are talking about their innovation economy and making this a focal point of their economic and strategic planning."*⁶⁴

The Body of European Regulators for Electronic Communications (BEREC) published a report in October 2015 (BoR (15) 142) which recognizes that *"technological developments, especially the transition to the IP technology, which enables a growing range of services to be consumed online, has implied the emergence of new services and business models operating over the Internet. The provision of Internet-based services commonly known as "over-the-top" (hereafter: OTT) is of increasing importance in the rapidly evolving information- and communication technology industry, and of great value for consumers and businesses. BEREC acknowledges that availability of OTT services is*

⁶¹ www.news.com.au/finance/economy/federal-budget/australians-to-pay-millions-more-for-digital-music-movies-games-and-apps-under-federal-budget-plan/news-story/7ac55733c877a0ca0a657ef226cb08c7

⁶² [www.ey.com/Publication/vwLUAssets/EY-Digital_products_and_services_in_2015/\\$FILE/Digital_VAT_Campaign_Brochure.pdf](http://www.ey.com/Publication/vwLUAssets/EY-Digital_products_and_services_in_2015/$FILE/Digital_VAT_Campaign_Brochure.pdf)

⁶³ www.irishtimes.com/business/economy/who-will-pay-europe-s-new-digital-tax-consumers-or-publishers-1.2052859

⁶⁴ Irene Ng, *The Innovation economy is here to stay ...*, 4 February 2016. Available at www.linkedin.com/pulse/innovation-economy-here-stay-irene-ng

also driving a change as for the competitive dynamics and technology scenarios in communication markets and, therefore, the BEREC 2015 Work programme has identified OTT development as a strategic area of investigation.”⁶⁵

Aside from the data protection and privacy issues, and the regulation of social media, the greatest challenge for ICT regulators is the optimal approach to OTT supervision and regulation (if any). There is no question that there are significant regulatory imbalances that currently exist between the approach both in law and by regulators in relation to traditional telcos compared with OTT providers. Such regulatory imbalances are summarised in Table 3: Regulatory imbalances between traditional and OTT operators below.

Table 3: Regulatory imbalances between traditional and OTT operators

Areas of Regulation	Network Operators	OTT Players
1. Applicable laws	Domestic law or in Europe EU regulations	Home jurisdiction maybe; many gaps in applicable laws
2. Taxes	Local and domestic taxes	Located in low cost locations and tax havens
3. Licensing	Must be granted or acquire licence from national Governments	Mostly exempt
4. Operating Area	Only serve customers within the jurisdiction	Serve any user globally
5. Infrastructure/ Network	Investing in new technology networks to deliver services to end users	No investments in networks that reach end users while telcos must deliver competitors services
6. Competition	Strict rules applying including ex ante & per se rules, M&A restrictions	Mostly exempt except M&A if OTT subject to domestic competition law
7. Fees	Customers' charges contribute to the costs of network provisioning	<ul style="list-style-type: none"> Services offered without any relationship to the underlying costs; two sided markets
8. Quality of Service	License requirements include SLAs and/or mandatory QoS standards	<ul style="list-style-type: none"> No QoS guarantee QoS issues blamed on network provider
9. Inter-connection	<ul style="list-style-type: none"> Required as part of regulatory regime Additional costs 	OTTs have no interconnection requirements for calling or messaging
10. Net neutrality	<ul style="list-style-type: none"> If applicable, best effort data transport without discrimination, independent of source or nature of data. Only typically traffic management permitted 	<p>No obligations (control over content and freedom of choice concerning customers)</p> <p>OTTs could be affected if Network operators apply traffic management restrictions</p>
11. Emergency services	Mandatory provisioning as part of licence conditions	Typically no such obligations
12. Interception	Strict regimes with costs borne by operator	Typically no such obligation

⁶⁵ http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/5431-draft-berec-report-on-ott-services_0.pdf.

	Areas of Regulation	Network Operators	OTT Players
13.	Retail Prices	Regulators' approval is typically needed in advance	No need for approval and maybe free for users
14.	Universal Service	<ul style="list-style-type: none"> • Mandated • USO contributions as a percentage or network revenues 	No contribution
15.	Spectrum fees	Required to acquire in an auction or pay market based fees for usage	No additional costs for OTT
16.	Privacy	Strict data protection and privacy requirements for users	Practiced on a limited and generally voluntary basis
17.	Number Portability	Obligation to offer number portability between providers	OTT service independent from mobile number

Source: Moktar Mnakri, *Regulating "Over-The-Top", Services - Need and Efficiency*, Arab Regional Forum on "Future Networks: Regulatory and Policy Aspects in Converged Networks". 19-20 May 2015 as augmented and modified by Windsor Place Consulting.

A number of other countries are looking at such issues and there have been international forums arranged by the ITU.⁶⁶ To highlight one market, in South Africa, the parliamentary Portfolio Committee is presently conducting an inquiry into data services and the possible impact of OTT providers on the market. In response, South Africa's network operators have requested the regulation and implementation of policies to govern OTTs, claiming the loss of a substantial portion of their revenues to new technologies. In order to produce a regime that is representative of the realities of the marketplace and technological landscape, the South African Government is attempting to balance multi-stakeholder objectives.

The approach taken by different regulators globally to OTTs has thus far varied. One regulatory trend has been to block the provision of OTT VoIP services. Alternatively, the regulatory approach in countries such as the UK and Australia has been to classify the different types of VoIP and treat them accordingly. Where VoIP services that are not designed to substitute directly for, or to interconnect with the PTSN, they are left unregulated. However, those that are designed to substitute traditional telephone services have been regulated with a 'light-handed' approach or when there was no specific regulatory framework for VoIP services they were classified and treated as any other telecom services.

Similar to earlier comments in this paper, the establishment of a "two-track" regulatory regime for legacy telcos and OTT providers in the ICT sector is neither sustainable nor optimal. Regulating fixed and mobile network operators differently from newcomers is likely to confer an unfair advantage to the model which has the least costly regulatory burden. Established network operators should not be punished for complying with the law and regulations, nor should new businesses be punished for offering innovative ICT services. Harmonizing regulations across the sector over time is optimal and arguably necessary as all industry sectors including the ICT sector are transformed.

⁶⁶ See ITU - ASEAN Forum on Over The Top (OTT) services, 8-9 December 2015. Phnom Penh, www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/Events/2015/Dec-OTT/en.aspx

Such harmonisation must however take account of the changed nature of competitive advantage, dominance and market power. Consequently, regulating OTT services as incumbent operators is not viable; nor is the continuation of current regulation on operators possible without change. The challenge is to adopt more collaborative regulatory measures where the applicable regulation on all market players is converged, coherent, promotes competition and provides incentives to invest and be innovative. Adopting only regulation which is necessary would seem to have considerable merit.

6.5.4 Competition concerns

In technology, today's small entrants are tomorrow's dominant firms. Witness the growth of players such as Google, Facebook and alike. While initially it may seem that the app economy promotes competition against legacy providers, there is a danger however, as these businesses grow, they may be tempted to utilise their market power⁶⁷ rather than compete. The economies of scale and scope are even more pronounced in the digital world.

As a consequence, the rise of the app economy does not alter the fact that competition policy should be at the heart of economic regulation in each and every market economy providing a set of tools to promote sustainable competition.

This means that competition regulators will need to be very watchful. In particular, the terms and conditions contained in contracts between sharing platforms and both suppliers and buyers need careful scrutiny especially if they involve exclusivity arrangements. This issue has been discussed earlier in this report.⁶⁸

Competition policy may be implemented through general competition laws, or through competition enhancing rules in specific sectors. In this context there is a need for a strong interworking arrangement between ICT regulators and general competition regulators, if they are separate. When there are separate entities enforcing telecommunications/ICT and competition rules, balancing the interplay and jurisdiction between these two entities is a key element in allowing the app economy to expand. On the other hand, where a single entity exists (either a Telecommunication/ICT regulator or a general competition authority), policies applicable to the sharing economy should encourage growth and competition.

⁶⁷ Market power occurs when an industry participant can unilaterally set and maintain prices and other commercial terms.

⁶⁸ It is also the subject of review by global competition regulators. The International Competition Network (ICN) conference held in Singapore from 26 to 29 April 2016 has as one its themes a special project entitled "*Dealing with Disruptive Technologies & Engaging Stakeholders: Challenges and Opportunities for Competition Agencies*". See <http://www.icn2016.sg/>. The ICN is the peak body devoted to national and multinational competition authorities. While the study/survey is not yet completed please refer to this presentation on its scope. www.oecd.org/competition/globalforum/Singapore_TOH%20Han%20Li_Disruptive%20Innovations.pdf

In addition to minimising an overlap between ICT and general competition regulators, if separate, it is also necessary to consider whether *ex ante* competition rules may be needed for some elements of the app economy in the future rather than rules which regulate *ex post* conduct (see Figure 28).

Figure 28: Is *ex ante* regulation needed in the future or is *ex post* regulation sufficient for regulating the app economy?

Ex post: After the event regulation relating to specific allegations of market abuse	Ex ante: Anticipatory intervention mainly concerned with market structure
Advantages: <ul style="list-style-type: none"> • Attempts to stop conduct only shown to be harmful • Lower information and monitoring requirements • Least disruptive regulatory approach for emerging markets 	Advantages: <ul style="list-style-type: none"> • Sets forward looking expectations for firm behaviour • Provides industry certainty by setting clear rules • Promotes a greater degree of transparency
Disadvantages: <ul style="list-style-type: none"> • Triggered only after anti competitive conduct has occurred • Securing information from accused firm is difficult • General competition provisions may be unsuitable for industry specific issues 	Disadvantages: <ul style="list-style-type: none"> • Can lead to excessive or unnecessary regulation • Can create market distortions through regulatory arbitrage • Regulatory processes are costly and prone to capture by regulated entities

Source: Windsor Place Consulting (www.windsor-place.com)

6.5.5 Net neutrality issues

In this context of the importance of the app economy, the issue of net neutrality⁶⁹ is also likely to be reassessed by global Telecommunication/ICT regulators. Net neutrality, file defined differently in various markets has at its core that that Internet providers should treat all network traffic the same, that providers should not block certain sites, apps or services, should not control access to certain sites, apps or services nor should they give preferential treatment to certain sites, apps or services.

The key issues under discussion globally, as to whether they are permitted and if so, to what degree, include:

⁶⁹ The BEREC's definition is that "literal interpretation of network neutrality, for working purposes, is the principle that all electronic communication passing through a network is treated equally. That all communication is treated equally means that it is treated independent of (i) content, (ii) application, (iii) service, (iv) device, (v) sender address, and (vi) receiver address. Sender and receiver address implies that the treatment is independent of end user and content/application/service provider."

- Traffic management. These include technical measures that allow network operators to allocate available resources and maintain QoS for all users across a network.
- Zero rating. Zero rating is the practice by Internet providers of offering customers access to particular apps, sites or services for free or without tapping into customers' limited monthly allocations of bandwidth. To make such an offer there is a business arrangement between OTTs and Telecommunications operators/Internet service providers.
- Differential pricing for data usage. Under this scenario, the Internet provider charges users different rates for the various apps and websites they use. Examples include the ability to price data differently, like how much data you have consumed (e.g. first 100MB free or at a higher/ lower rate) or the time of the day (e.g. free Internet during night hours).
- Bandwidth Throttling. Examples of this include the intentional slowing of Internet service by an ISP after data quotas have been exceeded (e.g. the first 8GB at 10mbps, and 512 kbps thereafter) or depending on type of application (e.g. VoIP). Often throttling on mobile networks occurs depending on whether users have complied with "acceptable use policies".

Internationally, three basic approaches to net neutrality issues in countries have been observed (see Table 4).

Table 4: Overview of approaches to Net neutrality

	Cautious observers	Tentative refiners	Active reformers
Measures taken	No specific measures	Light-handed NN measures: e.g. Guidelines or recommendations on transparency, lowering switching barriers, minimum QoS	Specific NN measures: e.g. laws in place, no blocking, no discrimination in treatment of traffic
Example countries	Australia Korea New Zealand (most of the countries)	Japan United Kingdom (voluntary code)	Argentina Benin Brazil (bill) Chile European Commission Ethiopia France India Mexico Netherlands Singapore Sudan Ukraine USA (FCC Order)

Source: ITU, 2015

It should be expected that a more active stance on the issue will be taken by ICT sector regulators. These approaches are:

- **Cautious observation:** These countries have taken note of net neutrality issues and have currently chosen not to take any specific measures to address these issues;
- **Tentative refinement:** These countries have adopted a light handed approach, with some refinements to the existing regulatory regime governing communications services, but not going so far as to prohibit certain behaviours; and
- **Active reform:** A growing number, these countries have gone further and sought to prohibit specific behaviours by ISPs, often subject to reasonable network management practices.

The GSR12 Best Practice Guidelines adopted by the global community of regulators recommend that regulators and policy makers seek to implement measures to oversee the use of traffic management techniques to ensure that those do not unfairly discriminate between market players. In addition, regulators also need to review existing competition laws to determine whether the regulatory tools, such anti-discriminatory law or regulations that are already in place, adequately address the competition issues that tend to impact net neutrality⁷⁰.

6.5.6 Possible approaches to licensing

App economy services are unprecedented in recent policymaking terms and in their pace of development, and how they will develop in the long term is difficult to predict. But if the benefits are real and the risks are manageable, then there's a good argument for legalising these services sooner rather than later so that they have a real chance to grow. This is easier said than done. Licensing structures in the telecommunications sector have been relatively static for some time, even though various attempts including by the ITU⁷¹ have been made to reform them. While perhaps licensing structures have underpinned by national WTO telecommunications sector commitments, in general licensing in the sector is focused on infrastructure and services typically with a number of sub-categories.

Alternative approaches, including those used in regulating the app economy in the transportation sector, may have broader merit in telecommunication/ICT sectors depending on the market and services concerned. They include:

- **Temporary licensing:** Apply temporary rules/grant licences for a limited period in order to permit greater study. This has been done in for example, Pennsylvania and Detroit, US, where Uber and similar services have classified these companies as 'experimental' service providers, in recognition of the fact that both their long-term impact and viability is unknown. These jurisdictions have given the

⁷⁰ GSR Best practices guidelines 2012 (https://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR12/consultation/GSR12_BestPractices_v3_E.pdf)

⁷¹ For example, see ITU, *Trends in Telecommunication Reform, 2004/05. Licensing in the Era of Convergence*.

companies temporary, two-year approval to operate while they decide on a more permanent regulatory response;

- **Transition arrangements:** Put in place transition schemes to compensate existing stakeholders. In the Australian State of New South Wales, UberX and similar services have been legalized, pending legislation in early 2016. They will be subject to an AUD1 levy per trip to fund a AUD250 million compensation package for the taxi industry. Some 50 taxi and hire car regulations were also repealed concurrently in that State.⁷² Such a levy provides funds for managing industry transition and compensating taxi plate holders; or
- **Deemed class licensing.** Another alternative approach which has been used in Singapore and has been debated in Malaysia and Indonesia is to use deemed class licensing for say web content such that services while not being located in the jurisdiction may be subject to a country's classification regime (eg with respect to nudity, violence etc.).

While such measures have not generally been adopted by telecommunication/ICT regulators except by the issuance of "no objection certificates" say, to a telecommunications operator's asset transfer ahead of later formal licensing⁷³ there would be merit for example, in having the ability to temporarily licence innovative services pending more detailed analysis or bring certain services within the penumbra of domestic regulation. New telecommunications legislation in selected jurisdictions would certainly permit this.⁷⁴ Putting in place transition from existing licensing and other sector regulatory regimes may also be required going forward.

Another approach which has considerable merit is industry or self-regulation. Industry regulation includes the formulation of industry codes of conduct. Often codes of conduct are industry-specific and will be decided by all operators or retailers within a given market amongst themselves. Examples of markets with a self-imposed code of conduct include the United Kingdom's ISP Code of Practice which is uniform and obligatory on all members.⁷⁵

The chief appeal of such regulation to providers is that, where sufficient self-regulation is accepted by market participants, regulators will not seek to impose more stringent rules. Regulators may also favour such mechanisms as they are flexible, can be implemented perhaps quicker than formal regulation and move the cost of regulatory compliance is with market players.

⁷² See www.smh.com.au/nsw/uberx-legalised-in-nsw-compensation-for-taxi-plate-owners-20151217-glpt6r.html

⁷³ For example, the no objection certificate issued by the Bangladesh Telecommunications Regulatory Commission (BTRC) in relation to the tower company spinoff (ie passive infrastructure transfer) to edotco Bangladesh from Robia Axiata Limited dated 15 January 2013.

⁷⁴ For example, the Cambodian *Law on Telecommunications 2015* promulgated 17 December 2015 provides in Article 17, for the licensing of operations (other than infrastructure and services) to be determined by Prakas of Telecommunications Regulator of Cambodia.

⁷⁵ See www.ispa.org.uk/about-us/ispa-code-of-practice/

6.6 Recommended approaches to regulation of the app economy

6.6.1 Overview

This report highlights the importance of the app economy, its speed and its transformation effects on broader economic activity.

It is important to appreciate that sharing economy sometimes involving two-sided markets is complex and very different from the traditional telecommunications markets. The traditional linear relationship between operator and subscriber may no longer exist and where it does, this relationship may not just be local but indeed global. Frameworks therefore must evolve as markets evolve, it is not possible to regulate the future into the past. In addition to technology neutrality, regulatory frameworks must also be as future-proofed as possible. Flexibility is arguably the key but there is little doubt that new arrangements, approaches and tools are likely to be necessary. As highlighted elsewhere in this report, some of those frameworks may need to be temporary and transitional.

Supporting innovation is not however the only goal. There are some elements of regulation which ought to be immutable. These pillars include the need for competition policy – both between competing substitutable services and in the supply of connectivity, consumer protection, data protection and privacy, and that the services supplied especially to consumers of are merchantable quality.⁷⁶ Taxation and the application of domestic laws on the international supply of services and content further highlight the complexity of this new environment and the upcoming challenges. The optimal approach to app or app economy does not mean more regulation but rather better regulation.

6.6.2 Building Blocks for App Economy Regulatory Guidelines

Given the above, the suggested advice to Government and ICT regulators in relation to future regulation in the Telecommunications/ICT sector is set out in Figure 29.

Figure 29: Suggested advice to Government and Telecommunications/ICT regulators

Undertake a review of the regulations applicable to network operators and OTT players: Assess whether such regulations are appropriate, whether forbearance should be applied to network operators, whether additional rules should apply to OTT providers and map how regulation of market participants – especially for substitute/competing services - should converge over time. Likewise review content regulation to ensure in a global market with greater levels of realism (e.g., virtual reality and similar) are appropriate and consistent with domestic conditions and cultural policy objectives. A key element of such a review is to

⁷⁶ In others words, “when the buyer, expressly or by implication, makes known to the seller the particular purpose for which the goods are required, so as to show that the buyer relies on the seller's skill or judgment, and the goods are of a description which it is in the course of the seller's business to supply (whether the seller is the manufacturer or not), there is an implied condition that the goods shall be reasonably fit for such purpose.” See *Sale of Goods Act, Queensland, 1896*, section 17. Available at http://www.austlii.edu.au/au/legis/qld/consol_act/soga1896128/s17.html

consider market definitions and whether such definitions currently permit a differentiated regulatory treatment for OTT services.

Update the licence conditions and as required provide deeming provisions for non-resident OTT providers etc.: Update analogue/legacy licence conditions so as to reflect the move to digital/IP services and as required enact legislative amendments to provide for deeming provisions (eg to be say, a special class licence) for non-resident OTT providers etc.

Assess and continually monitor the state of competition in the market. It is critical to assess and critically monitor the state of competition in ICT markets. Ensure there are no gaps in regulation between telecommunications regulators and general competition regulators including where services are offered from outside the jurisdiction. Promote competition whilst recognising that ICT services markets are no longer national and that there is a range of competing services which are domiciled domestically. Ensure that operators with significant market power do not foreclose or significantly dampen the innovative service offerings and OTT services. Further, acknowledge as outlined earlier in this paper that while initially they may have provided strong disruptive competition, as new digital businesses grow and scale almost exponentially, they may be tempted to exercise their market power. Regulators will need to be watchful that the digital economies of scale and scope are not exploited contrary to law.

Collaborate with tax authorities: Ensure that there is, to the extent possible a level playing field for competing services. Such analysis should include the applicable income and value added taxes applicable to competing services.

Promote and facilitate ubiquitous broadband: Recognising the political, economic and societal need for ubiquitous broadband formulate policies to facilitate nationwide broadband using a mix of cable/fibre, wireless, satellite and other technologies. In particular, given the growing importance of wireless broadband to the meeting of global broadband density targets that there is sufficient International Mobile Telecommunications ('IMT') spectrum of at least 760 MHz but preferably 840 MHz IMT spectrum available and allocated to such services by 2020. In addition, to promote investment in backhaul transmission and higher speed broadband services in urban/economically viable regions.

Ensure adequate and up to date data protection, privacy and cyber security legislation based on global exemplars: Ensure that domestic legislation for data protection, privacy and cyber security is based on global exemplars and that agencies charged with ensuring compliance and promoting education are properly resourced and staffed by experts. The scope of such legislation should be wide and include legacy and new systems including the Internet of Things ('IoT'). It is also critical to enact digital identification ('digital ID') legislation.

Establish co-ordination procedures between regulators: Establish co-ordination procedures between communications sector regulators and regulators of broadcasting/content (if separate), competition, financial services and privacy/data protection to ensure consistent regulation and comprehensive inter-working arrangements.

Engage in greater public awareness and advocacy campaigns in relation to digital/ICT services: It is important that the public including all sections and age groups in society are well-informed as to their digital rights and responsibilities.

Regulators must engage more broadly with education and training sector: As many skills needed in the future and indeed the jobs of the future are very different from today, there is a role for sector stakeholders lead by the regulator to engage with Education and training Ministries, universities, tertiary institutions, schools and other places of learning to ensure that curriculum and syllabus reflect the app economy and the move to a digital society.

7 APPENDIX A: DATA FOR THE APP ECONOMY

As noted in Section 6, the onset of the App Economy has prompted widespread industrial change. However, quantifying the scale and scope of these changes is difficult. Established metrics and categories that national governments use for data collection are not applicable to the App Economy. Further, the App Economy has various flow-on effects within constituent ecosystems that present a fundamental problem for traditional modes of measurement. Almost every industry in the traditional economy is rapidly spilling revenue into the App Economy, as apps are integrated into existing modes of consumption.⁷⁷ Applicable data sources are fragmented, and often not particularly comprehensive on comparable points.

This report summarises data on the most obvious available economic indicators of the App Economy. A core component of findings relate to labour market data. In this report, 'App Economy jobs' are defined so as to include:

- Core ICT App Economy jobs: ICT-related jobs that use App Economy skills: the ability to maintain, develop, or support mobile applications. These include app developers, software engineers, and security engineers; and
- Direct non-ICT App Economy jobs: non-ICT jobs (such as HR, marketing or sales) that supports core App Economy jobs in the same enterprise; and
- Indirect or 'spillover' job: roles that exist to support workers in app development, production, marketing, and sales of apps or app-related products.
- Indirect ICT jobs: at telcos, etc. traditional players providing network services for mobile broadband and which have operations (supporting or else) to the app economy.

Further, to complement limited economic data, this report notes qualitative findings, and other indicators of the broader industrial effects of the app economy, where relevant. This report notes that the ITU may wish to consider accessing commercial data sources for further quantitative information as required.

7.1 Comparative global data

In 2016, the global mobile app market is projected to expand 24 percent to reach \$51 billion in gross revenue across all app stores. By 2020, gross revenue across all app stores will exceed \$101 billion globally. China will surpass the U.S. in terms of total revenue from app stores by the first half of 2016, having surpassed it in downloads in early 2015. Mature markets will see continued growth, while emerging markets like India, Indonesia,

⁷⁷ Vision Mobile, 2015, 'European App Economy 2015: Creating jobs and driving economic growth in Europe', www.visionmobile.com/product/european-app-economy-2015/

Brazil, Argentina and Turkey will expand the most dramatically this year and through 2020.⁷⁸






Table 5: Top 25 countries of app use, ranked by Smartphone users, 2013-2018 (millions)

Country	2013	2014	2015	2016	2017	2018
1. China	436.1	519.7	574.2	624.7	672.1	704.1
2. US	143.9	165.3	184.2	198.5	211.5	220.0
3. India	76.0	123.3	167.9	204.1	243.8	279.2
4. Japan	40.5	50.8	57.4	61.2	63.9	65.5
5. Russia	35.8	49.0	58.2	65.1	71.9	76.4
6. Brazil	27.1	38.8	48.6	58.5	66.6	71.9
7. Indonesia	27.4	38.3	52.2	69.4	86.6	103.0
8. Germany	29.6	36.4	44.5	50.8	56.1	59.2
9. UK	33.2	36.4	39.2	42.4	44.9	46.4
10. South Korea	29.3	32.8	33.9	43.5	35.1	35.6
11. Mexico	22.9	28.7	34.2	39.4	44.7	49.9
12. France	21.0	26.7	32.9	37.8	41.5	43.7
13. Italy	19.5	24.1	28.6	32.2	33.7	37.0
14. Turkey	15.3	22.6	27.8	32.4	37.2	40.7
15. Spain	18.9	22.0	25.0	26.9	28.4	29.5
16. Philippines	14.8	20.0	24.8	29.7	34.8	39.4
17. Nigeria	15.9	19.5	23.1	26.9	30.5	34.0
18. Canada	15.2	17.8	20.0	21.7	23.0	23.9
19. Thailand	14.4	17.5	20.4	22.8	25.0	26.8
20. Vietnam	12.4	16.6	20.7	24.6	28.6	32.0
21. Egypt	12.6	15.5	18.2	21.0	23.6	25.8
22. Colombia	11.7	14.4	16.3	18.2	19.7	20.9
23. Australia	11.4	13.2	13.8	14.3	14.7	15.1
24. Poland	9.4	12.7	15.4	17.4	19.4	20.8
25. Argentina	8.8	10.8	12.6	14.1	15.6	17.0

Source: eMarketer 2014

⁷⁸ http://blog.appannie.com/app-annie-releases-inaugural-mobile-app-forecast/?utm_source=AAhomepage_LO&utm_medium=cta_button&utm_campaign=1602_App_Forecast

Figure 30: Global App Economy – platform comparison⁷⁹

	 ANDROID	 iOS	 HTML5 MOBILE	 WINDOWS PHONE	 BLACK BERRY 10
Sales market share (smartphones, Q3 2013)	81%	13%	-	4%	2%
Mindshare	71%	55%	52%	26%	14%
Priority	37%	32%	14%	6%	5%
Loyalty	52%	59%	26%	24%	35%
Most popular in	Asia	North America	South America	Asia	South America
Median revenues	\$150	\$750	\$150	\$25	\$75
Differentiating selection criterion	Open Source	Revenue potential	Ease of porting	Choice of development environment	Documentation/ Access to hardware APIs
3rd party tools index	2,8	3,1	2,5	2,5	2,3
Top revenue model	Advertising	Contract development	Contract development	Advertising	Pay per download
Segments with a strong preference to the platform	Hobbyists, Gold Seekers	Digital Media Publishers, Hunters, Guns for Hire	Product Extenders, Enterprise IT	Hobbyists, Explorers	-

Source: Vision Mobile via TheAPPY 2014

Below is a discussion of data on a regional and national basis, indicative of the global economic significance of the App Economy.

7.2 Europe

The European⁸⁰ mobile App Economy market is continuing to grow on a rapid trajectory. User bases are increasing, as smartphone penetrations rates reached 50% of mobile users in 2015.⁸¹ Consumers are fuelling the corresponding increase in app development markets. However, future growth will be met with the limitations of potential market saturation, and offshore competition - particularly from Asia.

⁷⁹ www.theappys.ie/blog-news/global-app-economy-will-be-worth-143-billion-by-2016/

⁸⁰ Note: references to Europe here include EU member states, plus Switzerland and Norway

⁸¹ ITU.

7.2.1 Employment

Currently, it is estimated that there are between 1.6 – 2 million App Economy jobs in Europe.⁸² The app development industry is estimated to have earned developers in Europe over 11 billion USD from around the world.⁸³ Two-thirds of these roles belong to full-time professionals. This is indicative that the European market has maintained its global standing and is relatively stable, even in light of increasing Asian competition.

Of these developers, a study by *Vision Mobile* estimates that for every app developer job in the EU, an additional 1.31 non-technical and indirect jobs are created on average.

Figure 31: Vision mobile: 2 million App Economy jobs in EU28, 2015⁸⁴



Source: Vision Mobile 2015

7.2.1.1 Drivers of employment

iOS and Android generate most of these non-technical jobs. Notably, there are more professional developer jobs tied to iOS (40%) app development than to Android (33%). This speaks to the nature of the mobile user market in the region: Apple products continue to be the preferred platform in the region. In 2016, Apple announced it was opening Europe's first iOS app development centre in Italy. The centre will support teachers, and create a specialized curriculum for developers.⁸⁵

However, the total proportion of app-related employment directly attributable to iOS has fallen. This is presumed to be due to the maturing of the EU app development market, with corporations supporting parallel development in iOS and Android to cover entire

⁸² Note – estimates based on Vision Mobile 2015 report, and Progressive Policy Institute paper (2016). The latter used a considerably more conservative ratio estimate metric, hence the discrepancy in results. See:

www.progressivepolicy.org/blog/app-economy-jobs-in-europe-part-1/
www.visionmobile.com/product/european-app-economy-2015/

⁸³ www.apple.com/pr/library/2016/01/21Apple-Opening-Europes-First-iOS-App-Development-Center-in-Italy.html

⁸⁴ As noted, the 2016 *Progressive Policy Institute* papers use a more conservative ratio estimate. The *Vision Mobile* estimates remains useful as indicators of relational aspects of the industry.

⁸⁵ www.apple.com/pr/library/2016/01/21Apple-Opening-Europes-First-iOS-App-Development-Center-in-Italy.html

mobile user markets. Other platforms, including Windows Phone and its mobile browser, also create jobs, albeit at a much lower multiplying rate.

7.2.1.2 Policy response

European politicians are also starting to take an increased interest in the sector. Policies and programs are being put in place to support future App Economy innovation, and development. For instance, the Startup Europe program aims to offer an integrated pan-European platform to help startups and entrepreneurs. The initiative works by pairing top startups with corporate participants, to help startups emerge more rapidly from local ecosystems and economies of scale.⁸⁶

7.2.1.3 Incomes

The average incomes of App Economy jobs in Europe also surpass their regional and global market equivalents – pointing to the stability and security of the EU app developer market. In the EU, more than half (51.4%) of app developers make over \$500 per month, over the worldwide average of 48.7%. Notably, enterprise app developers in Europe earn significantly more than their consumer-based counterparts. A survey of full-time App Economy professionals reveals that 47% of developers making enterprise apps earn more than \$5,000 per month, while only 32% of consumer app developers exceed this level.

7.2.1.4 Dominant national markets

France, Germany and the UK are among the top app producing markets in Europe. As a percentage of total workforce, App Economy jobs are estimated to represent 0.9% in France, 0.7% in Germany, and 1.0% in the UK. The Nordic countries are also emerging, with lower numbers of jobs that make up a higher percentage of smaller labour markets.

⁸⁶ <http://startupeuropepartnership.eu/>

Table 6: App Economy jobs by European country: by total number and as % of overall labour market⁸⁷

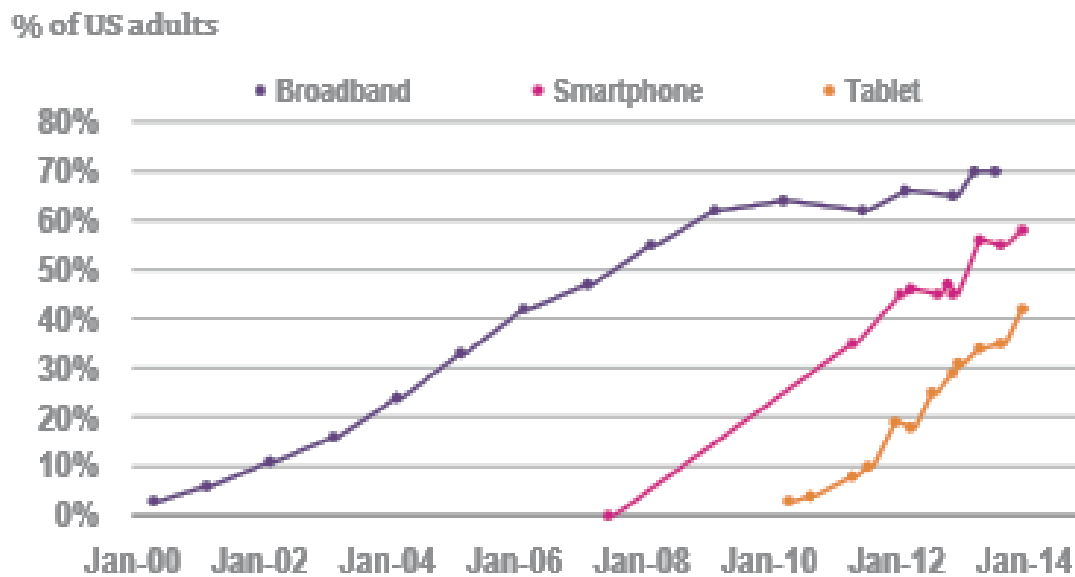
Country	No. of jobs (1000s)	% of overall labour
UK	321.2	1.0%
Germany	267.9	0.7%
France	228.9	0.9%
Netherlands	125.2	1.5%
Italy	97.5	0.4%
Poland	84.3	0.5%
Spain	78.2	0.5%
Sweden	67.2	1.4%
Finland	47.4	1.9%
Norway	41.6	1.6%
Denmark	33.4	1.2%
Switzerland	28.5	0.6%
Portugal	27.4	0.6%
Belgium	23.4	0.5%
Czech Republic	19.2	0.4%
Hungary	15.3	0.4%
Ireland	13.2	0.7%
Austria	11.9	0.3%

7.3 USA

The American app market was valued at USD87 billion in 2014, and is projected to grow to 150 billion by 2017. The rates of smartphone adoption in the US are increasing to the point where smartphone use will outstrip broadband access. The App Economy in the US is only set to grow larger, with 37% the current estimates of approximate annual growth rate.

⁸⁷ www.progressivepolicy.org/blog/app-economy-jobs-in-europe-part-1/

Figure 32: App Economy technology adoption in the US



Source: Plum Consulting, Pew Internet Research

7.3.1 Employment⁸⁸

An estimated 1.66 million app economy jobs exist in the USA in 2016. The App Economy is cited as a significant driver of the growth in the US economy since the development of smartphones and app platforms in the nation in 2007-2008. 22.7% of App Economy jobs are predictably located in California, with the next-largest App Economy states being New York (9.4%) and Texas (7.3%). It is worth noting that the App Economy has spread widely from its birthplace in Silicon Valley, to 25 other states in the country. This evinces the decentralisation of app development, and related employment.

Table 7: Estimates of American App Economy jobs over time

Publication	App Economy jobs (1000s)
Feb 2012	466
October 2012	519
July 2013	752
Dec 2015- Jan 2016	1660

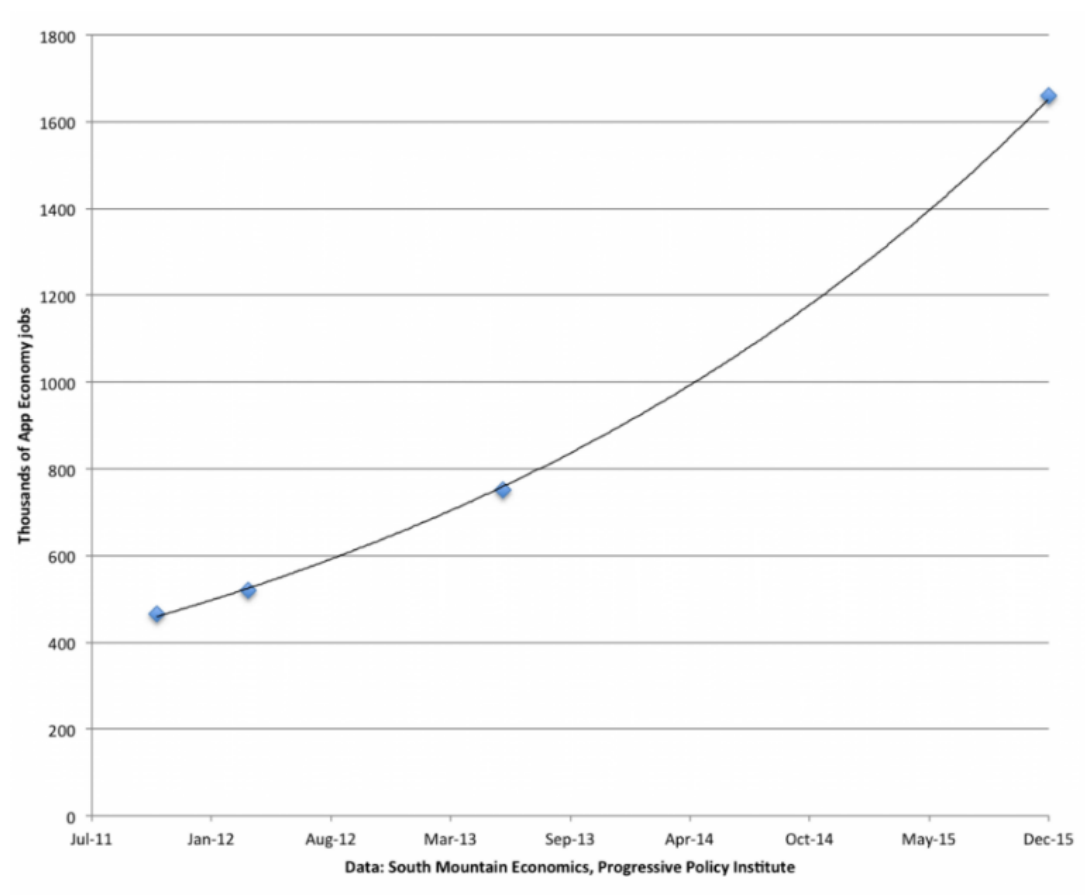
Source: Progressive Policy Institute synthesis of South Mountain Economics, The Conference Board, Indeed, and BLS data.

⁸⁸ www.progressivepolicy.org/blog/app-economy-jobs-part-2/

7.3.1.1 Drivers of employment

Small companies and startups comprise of 77% of the American app industry, dominating larger players in all categories except gaming. As with Europe, iOS and Android systems dominant the App Economy markets. iOS developers have experienced a 54% job growth between 2012-2014, while Android has experienced 110% job growth. This rapid increase in Android developers is likely to be for similar reasons to comparable growth in Europe. That is, with the maturing of the American app development market, entities are now supporting parallel development in iOS and Android to cover entire mobile user markets.

Figure 33: Growth trajectory of American app economy



Source: Progressive Policy Institute

Table 8: Market comparison: Europe vs the US⁸⁹

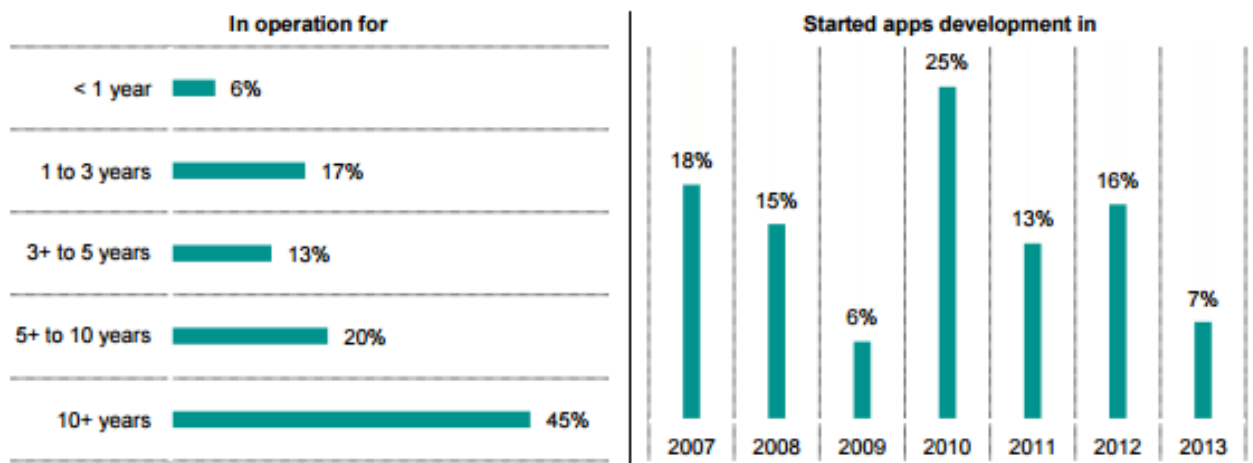
	App Economy jobs (millions)	As % of overall labour market
Europe	1.64	0.7%
United States	1.66	1.2%

Source: Progressive Policy Institute

7.4 Canada

The Canadian app market has been on a growth trajectory in recent years. The total number of apps users in Canada is 18 million, as smartphone penetration rates are set to exceed 21 million.⁹⁰ An estimated half of all Canadian businesses use mobile technologies to input data for faster information flows.⁹¹ Entities developing apps are generating \$1.7 billion in revenue per year, a figure expected to climb to CAD3.3 billion in 2017, and CAD5.2 billion by 2019. However the recent economic downturn in the nation has affected app sales, and initial forecasts are less certain than previously estimated.

Figure 34: History of Canada's App enterprises



Source: Surveys for Canada's apps enterprises, ICTC 2014

7.4.1 Employment

An estimated 64,000 jobs in the App Economy exist in Canada. Of these, 27,100 individuals are in technical positions, 24,100 are in non-technical roles, and 12,800 are in induced employment. This figure is predicted to grow to 110,000 by 2019. Estimated that

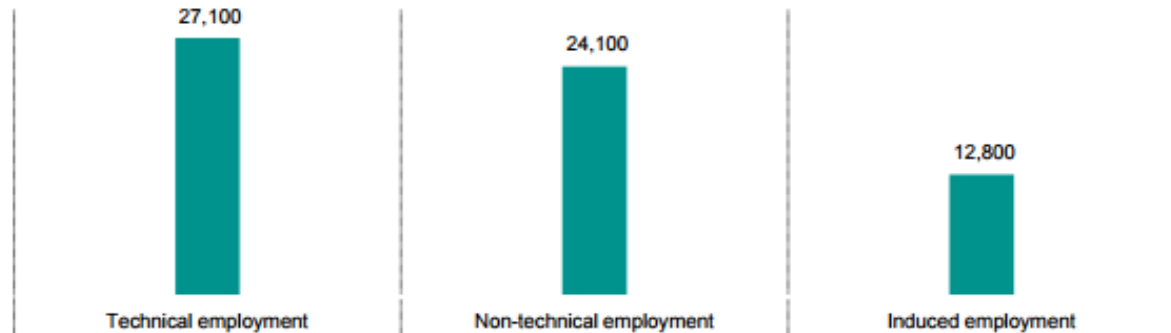
⁸⁹ www.progressivepolicy.org/blog/app-economy-jobs-in-europe-part-1/

⁹⁰ www.ictc-ctic.ca/wp-content/uploads/2014/02/AppificationFeb2014.pdf

⁹¹ *ibid.*

1 in 2 jobs is a technical position, the other a non-technical position assisting with promotion, marketing or sales.⁹²

Figure 35: Apps economy employment in Canada by job type



Source: ICTC 2014

7.4.2 Market

Canada's apps market faces many challenges. Global industry competition, lack of awareness of services offerings, shortages of capital, limited opportunities to collaborate with end-user enterprises and a shortage of skills all represent key impediments to future market growth.⁹³

Notably, the US is a key market for Canadian apps sales, as over a quarter (28%) of revenue is sourced from the US alone (see Figure 36). As the Canadian economy slows and exchange rates decreases the value of the Canadian dollar relative to the USD,⁹⁴ the Canadian app market will need to ensure within-province revenue streams remain stable. Notably, Apple's App store has introduced a new, lower pricing tier for apps in Canada in January 2016. The new tier will let developers price apps as low as CAD\$0.99, allowing developers to sell more copies of their apps, with less money for each sale.⁹⁵

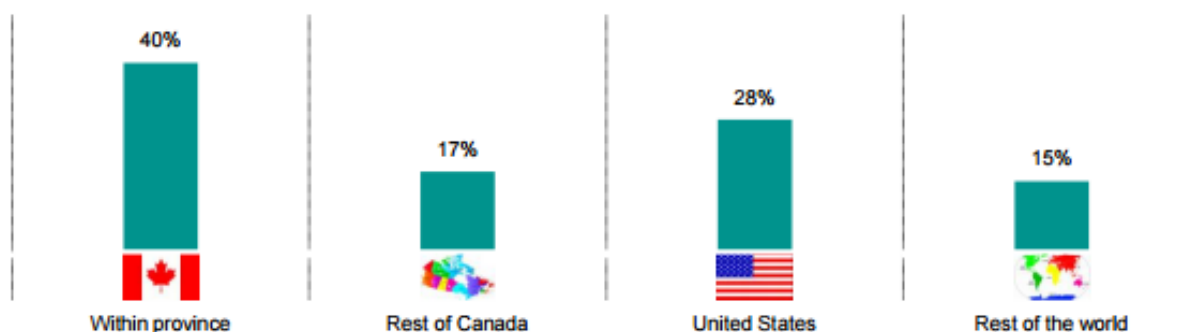
⁹² ibid.

⁹³ ibid.

⁹⁴ <http://mobilesyrup.com/2016/01/28/apple-introduces-new-0-99-pricing-tier-for-apps-in-canada-and-new-zealand/>

⁹⁵ ibid.

Figure 36: Revenue sources for Canada's apps enterprises



Source: Surveys for Canada's apps enterprises, ICTC 2014

7.5 India

The Indian mobile market has rapidly grown, to now include close to a billion mobile subscribers. Despite a relatively low smartphone penetration rate (est. 10% of total mobile users), and low internet penetration (17.4%, lowest among the BRICS) the aggregate number of smartphone users in India (100,000,000 approx.) still forms a large market for app downloads. For instance, India is among the top 5 countries for Google Play downloads internationally.⁹⁶

7.5.1 Developing market

As mobile data plans become more affordable and India's burgeoning middle class grows, the Indian app market is only set to grow further. However, India notably represents an opportunity for alternate OS platforms, particularly those designed to operate on lower-end devices. In this respect, India is distinct from developed markets where the Android/Apple duopoly is firmly established.⁹⁷ India is a highly price-sensitive market, and represents a challenge to OS companies and app developers to monetizing its large download market.

7.5.2 Employment

India currently hosts an estimated 75,000 'core' developers according to a study by the Indian Council for Research on International Economic Relations (see Figure 28 below for infographic of summary of study data). India is therefore the largest developer industry outside the USA. The aggregate number of jobs that the app market will create in India during the period 2014-16 is predicted to lie between 91,486 and 604,867. Notably the upper limit is close to eight times the current levels of employment. It is estimated that 10% of apps globally are developed by Indian nationals.⁹⁸

7.5.3 Social outcomes

The rapid growth of the app market in India is having a transformative impact on livelihoods and businesses. However, the potential for India to leverage the app

⁹⁶ <http://icrier.org/pdf/appreport.pdf>

⁹⁷ *ibid.*

⁹⁸ *ibid.*

ecosystem to achieve certain developmental goals is still underutilised. Current app usage in the nation is geared towards social networking and entertainment. Apps that focus on development initiatives like agriculture, health and education have not scaled adequately because of the limited nature of the Indian app ecosystem itself.

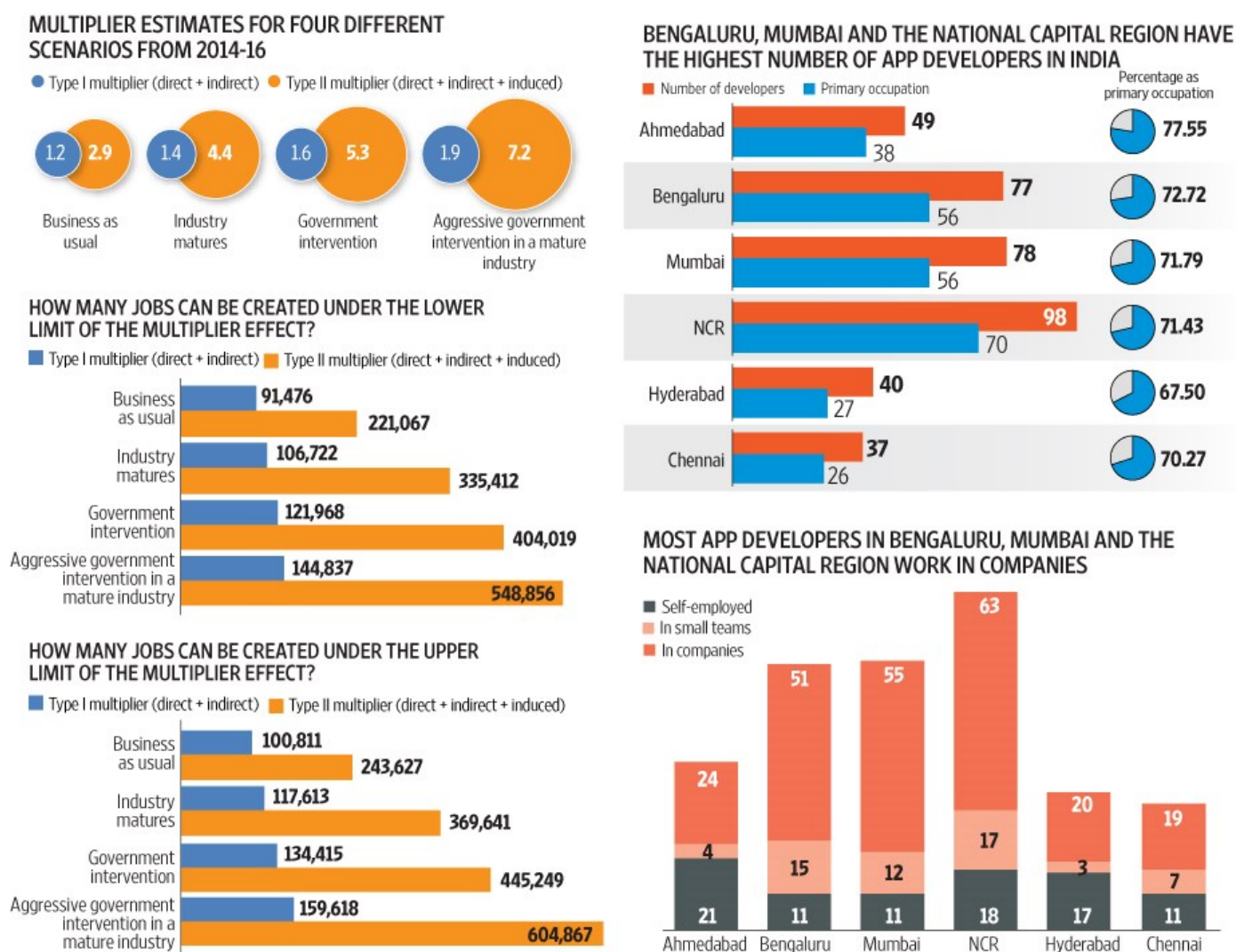
7.5.4 Policy responses

Notably, the Indian government has commenced its 'Mobile Seva' project to respond to the emergence of the nation's mobile market, and develop a framework of 'm-governance'. The Department of Electronics and Information Technology has developed a centralized mobile App store, currently hosting over 700 apps. The eGov AppStore facilitates public service provision via a common platform.

The eGov AppStore is hosted on the National Cloud, with apps customized so they can be used by government agencies and departments at Centre and State levels.⁹⁹ The eGov AppStore represents an interesting marriage of policy and developing market technology. If successful, the eGov Appstore will hallmark the capability of developing national governments to harness mobile markets to improve social outcomes.

⁹⁹ *ibid.*

Figure 37: Jobs and India's App Economy, 2015



Source: Livemint 2015 – based on research from Indian council for Research on International Economic Relations

7.6 Australia

The Australian App Economy represents is one of the most matured digital ecosystems internationally. Australia currently has a higher proportion of 'core' App Economy jobs as a share of all ICT roles than the United States and the United Kingdom.¹⁰⁰ Smartphone penetration rates in Australia are also higher per capita than in many international counterparts, including the US and the UK.¹⁰¹ It is estimated that Australia's computer systems design industry has grown at 38% since 2008, vastly outstripping overall employment growth.¹⁰² As the sector continues to grow, pundits highlight the potential

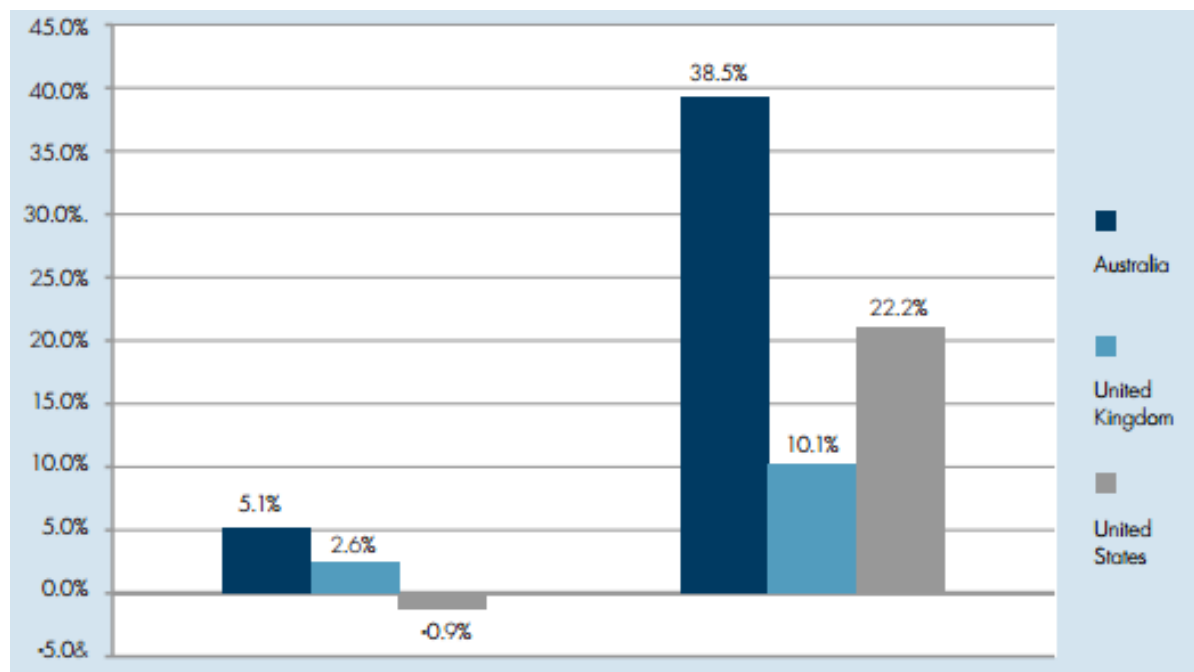
¹⁰⁰ www.acs.org.au/news-and-media/news/2014/jobs-in-the-australian-app-economy-white-paper-by-michael-mandel

¹⁰¹ http://landing.deloitte.com.au/rs/deloitteaus/images/Deloitte_Mobile_Consumer_Survey_2014.pdf

¹⁰² www.progressivepolicy.org/wp-content/uploads/2014/07/2014.07-Mandel_Jobs-in-the-Australian-App-Economy.pdf

for Australia to become an exporter of apps and app-related services, given the current international importance of English-language markets.

Figure 38: Australia's tech employment outperforms United States and United Kingdom (L: tech/info, R: computer systems design) ¹⁰³



Source: Progressive Policy Institute 2014

7.6.1 Features of a mature market

The Apple-Samsung duopoly is well-established in the Australian market. Australia has been a relatively early adopter of mobile payment and banking services and applications, and in-app usage rates are high.¹⁰⁴

Indeed, Australians spend an estimated 1 hour per day on in-app smartphone usage. However, app re-engagement rates are low. One attribution provider in the Australian market, Tune, has noted that only 13% of users remain active beyond a week of installing an app. Market leaders like Facebook and Google have responded rapidly to improve re-engagement, by releasing new ad products in 2015, and facilitating deep linking and post install measurement.¹⁰⁵

7.6.2 Employment

Approximately 140 000 workers are employed in the Australian app economy. On a per-capita basis, Australia compares favourably with other developed nations for App Economy employment and growth. As highlighted above, the computer systems design

¹⁰³ ibid.

¹⁰⁴ http://landing.deloitte.com.au/rs/deloitteaus/images/Deloitte_Mobile_Consumer_Survey_2014.pdf

¹⁰⁵ www.bandt.com.au/featured/future-app-economy-australia

industry comprises of 1.6% of overall employment in Australia (versus 1.2% of the US workforce).

Commentators have also noted the potential for digital economy-industries to supplement the flagging resources sector in the nation.¹⁰⁶ Employment in Australian computer systems have risen 38% since 2008, as compared with 8% in the rest of the economy. By way of international comparison, the US has seen a 22% gain in computer systems employment, versus 10% in the UK. Also notably, NSW is Australia's largest source of App Economy jobs, with 77, 000 employees working in the sector.

7.6.3 Vietnam

Vietnam is noteworthy for having the top-rated App Economy in Southeast Asia (see Figure 30 below). Vietnam has a fast-growing number of app developers. The use of apps in the country is only set to continue, as smartphone penetration rises and individuals use of mobile apps increases. The Vietnamese government is seeking to support industry growth by sponsoring initiatives like 'Vietnam Silicon Valley' - a group intended to help the growth of startups.¹⁰⁷

7.6.4 Employment

There are currently 29,000 App Economy jobs across the country¹⁰⁸. However, app developers who are using Vietnamese workers often are building apps that appear in other countries. The Japanese-based app developer company 'Mulodo' has an office in Ho Chi Minh City, as does Singapore-based entities Hoiio and Vinova. Multinational companies are also using Vietnamese workers to develop applications and software in their supply chains.¹⁰⁹

¹⁰⁶ www.progressivepolicy.org/wp-content/uploads/2014/07/2014.07-Mandel_Jobs-in-the-Australian-App-Economy.pdf

¹⁰⁷ www.progressivepolicy.org/wp-content/uploads/2015/09/2015.09-Mandel_Vietnam-and-the-App-Economy1.pdf

¹⁰⁸ *ibid.*

¹⁰⁹ *ibid.*

Table 9: Vietnam: leading the app economy

Vietnam's App Economy Leads Southeast Asia	
Country	SE Asia App Economy Index, adjusted for omitted job postings*
Vietnam	1.83
Singapore	1.37
Indonesia	1.37
Philippines	0.90
Malaysia	0.75
Thailand	0.35

**SE Asia App Economy index = number of job postings containing terms 'iOS' or 'Android' for that country divided by the average number of job postings containing terms 'iOS' or 'Android' for all six SE Asia countries. Indonesia and Malaysia data adjusted to eliminate spurious results from one job board. Index except for Vietnam adjusted for omitted job postings.*

Data: Indeed summary job postings, collected as of August 5, 2015, analyzed by the Progressive Policy Institute. Based only on publicly available data—no personal individual or business data used.

Source: Progressive Policy Institute 2015

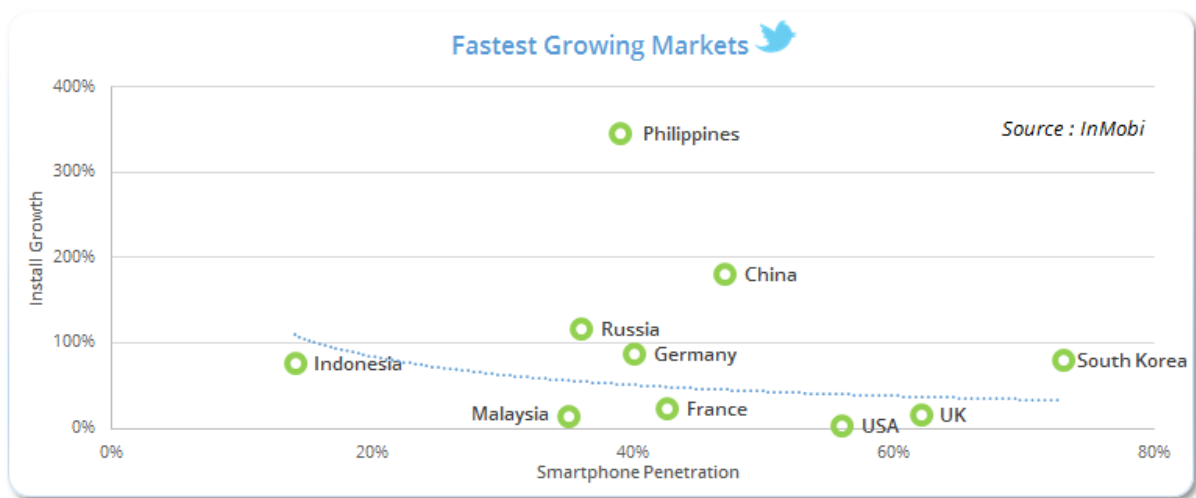
7.7 Indonesia

Indonesia's App Economy is relatively under-developed. Nevertheless, the number of developers in the country are beginning to increase. It is estimated that there are 22,000 App Economy jobs across the country¹¹⁰. Despite low current smartphone penetration rates, audiences are eager to download and install apps. As smartphone penetration rates increase, the Indonesian App Economy will develop further. Indonesia is marked as a significant growth market, noted as one of the most upcoming app install destinations of the world.¹¹¹ (see Figure 39).

¹¹⁰ www.progressivepolicy.org/wp-content/uploads/2015/09/2015.09-Mandel_Indonesia-Road-to-the-App-Economy.pdf

¹¹¹ www.inmobi.com/blog/2015/04/16/inmobi-insights-the-dynamics-of-a-booming-app-economy

Figure 39: Smartphone Penetration and Install Growth



Source: InMobi 2015

7.8 Belarus

7.8.1 6.9.1 Developing market

Despite a struggling economy and a restrictive political environment, Belarus has become a top performer in the IT sector, with the value of its companies' exports reaching over USD800 million in 2015.¹¹²

Testifying the growth of the Belarusian app economy, Facebook recently acquired Masquerade Technologies, a young Belarusian start-up whose live photo filters and face-swap technology picked up 15 million users in just three months. This is the fifth acquisition of a Belarusian high-tech firm by a notable foreign giant, another notably acquisition being popular instant messaging and VoIP app Viber by Rakuten.¹¹³

Employment

The turning point for the IT industry in Belarus came in 2005 when the government set up its Hi-Tech Park (HTP), a new hub established to promote the information and software development industry. Due to the legislative initiative of the Belarus government, IT companies in this hub are exempt from all corporate taxes, including value-added tax, profit, real estate and land taxes.¹¹⁴

As of 2014, there were 106 companies in the park, employing roughly 12,500 app developers. As of 2016, there are 152 companies registered as HTP residents, with more than half being foreign companies and joint ventures. Notably, most of the residents of

¹¹² <http://phys.org/news/2015-12-programmers-boom-belarus.html>

¹¹³ www.spiegel.de/international/world/the-minsk-tiger-lukashenko-s-high-tech-ambitions-for-belarus-a-668405.html

¹¹⁴ www.park.by/

the park largely act as foreign sub-contractors for their Western counterparts, rather than as full-cycle IT product developers.¹¹⁵

The app developers that work in this hub enjoy a wide range of perks. In a decade, their monthly salary at the tech park has risen from \$236 to \$2,000, significantly higher than other countries in the region. The employees also pay a fixed lower rate of income tax and receive Western-style benefits packages. It is hoped by the Belarusian government through these incentives that the HTB hub will be comparable to Silicon Valley in the USA.¹¹⁶

7.9 Brazil

7.9.1 Developing market

Brazil's smartphone user base is estimated at 89.5 million, the 5th largest in the world, and is growing at an annual rate of around 22% per year. Additionally, Brazil is expected to grow app revenue 40% in 2016 despite an increasing economic slowdown in other sectors, a trend reminiscent of the strength of the U.S. smartphone and app market during the Global Economic Crisis of 2008.¹¹⁷

As of 2015, there are 138 app developing companies in Brazil, with a majority only present in their own domestic market. However, despite a growing app marketplace with many start-ups gaining increasing market awareness, a true app ecosystem is yet to form in earnest in Brazil.¹¹⁸ These app developers are still in their infancy in terms of revenue generation, with Brazilian smartphone users downloading apps largely from foreign developers. Certainly, the whole of Latin America contributes only minimally to the total world app market value.¹¹⁹ These facts may be attributed to issues around poor data network quality, consumer trust, low credit card penetration rates and a lack of skilled-labour to supply the local app economy in Brazil. Despite these trends, it has been argued that the volume and scale that the Brazilian market offers positions them as one of the most important markets for growth globally.¹²⁰

¹¹⁵ Ibid.

¹¹⁶ www.spiegel.de/international/world/the-minsk-tiger-lukashenko-s-high-tech-ambitions-for-belarus-a-668405.html

¹¹⁷ <http://venturebeat.com/2016/02/10/the-app-economy-could-double-to-101b-by-2020-research-firm-says/>

¹¹⁸ www.mobileecosystemforum.com/2015/04/28/10-things-you-need-to-know-about-the-mobile-market-in-brazil/

¹¹⁹ Ibid.

¹²⁰ www.idgconnect.com/blog-abstract/14241/app-economy-research-poorer-countries-losing

8 APPENDIX B: THE LARGE APP ECONOMY PLAYERS

8.1 Introduction

In this section, thirteen (13) companies part of the app economy have been selected and analysed, with more in-depth case summaries of each provided in Appendix B.

These cases have been chosen due to their dominance in a regional marketplace, on a global scale, or due to their disrupting capabilities. Each company's area of focus alongside its key metrics has been outlined in the tables below. This section highlights matters that are important to acknowledge in formulating an approach to the regulation of the app economy.

8.2 Global Market Titans

Table 10: Listing of Global Market Titans

Name	Area of focus	Key Metrics
Apple	iOS App Store	<ul style="list-style-type: none">World's largest information technology companyApp Store generated approximately USD6 billion in operating profit for Apple in 2015
Google	Android App Store	<ul style="list-style-type: none">Apple App store's main competitor200 million app downloads in 2015, largely driven by Android's growth in emerging markets such as Brazil, India and Indonesia
Facebook	Social Media Platform	<ul style="list-style-type: none">Most ubiquitous social network with more than one billion active users daily from around the worldMarket capitalisation of approximately USD294 billion in 2015

8.3 Market disrupters

Table 11: Listing of Market disrupters

Name	Area of focus	Key Metrics
Uber	Transport/Ride-Sharing	<ul style="list-style-type: none"> Valued at over USD60 billion 5 billion worth of venue in 2015 Currently does not make a profit due to marketing, driver incentives and cost of legal and regulatory disputes
Airbnb	Accommodation	<ul style="list-style-type: none"> As of May 2015, Airbnb has over 1.4 million properties available for tenants Not publicly traded, however its valuation as of its last funding round was USD24-25 billion.
Skype	Social media & communication platform including instant messaging, video chat and VoIP	<ul style="list-style-type: none"> Acquired by Microsoft in 2011 for USD8.5 billion As of 2014, estimated that Skype accounts for 40% of all international calling
Netflix	Movie and television online streaming	<ul style="list-style-type: none"> Over 74 million subscribers As of January 2016, Netflix can be accessed in 130 countries Revenue of approximately USD6.1 billion in 2015
iSignthis	Identity verification for online transactions	<ul style="list-style-type: none"> Services are available to more than 3 billion customer accounts across more than 200 countries Best performing small cap on the ASX in 2015
Tencent	Internet conglomerate providing services such as instant messaging, online games, and taxi hailing	<ul style="list-style-type: none"> Largest internet company in Asia by market capitalisation at USD184 billion One of the largest instant messaging platforms globally, with peak simultaneous usage exceeding 100 million active users on more than one occasion

8.4 Regional Market Exemplars

Table 12: Listing of Regional Market Exemplars

Name	Area of focus	Key Metrics
Alibaba	E-commerce	<ul style="list-style-type: none"> Market capitalisation over USD200 billion, making it one of the largest companies globally as well as in its home market of China One of the world's most visited websites
Flipkart	E-commerce	<ul style="list-style-type: none"> India's biggest electronic commerce company Services available exclusively to India Estimated valuation of USD15.5 billion at the end of 2015
LINE	Instant Communication	<ul style="list-style-type: none"> Used globally, however most dominant in Japan, Thailand and Taiwan. LINE's revenue for 2015 is expected to exceed USD800 million
SocietyOne	'Peer-to-peer' lender	<ul style="list-style-type: none"> Based in Australia Facilitated loans worth AUD30 million by May 2015 SocietyOne's revenue is approximately 5 percent of the loans originated

8.5 Conclusions related to the case studies

A brief outline of these three categories of app-economy companies highlights issues that should be reflected in an approach to regulation of the app-economy. All companies chosen are vastly popular and successful, reflecting the immense benefit to consumers that their new and innovative services provide.

However, each are disrupting in their own sense, whether that be transcending borders, dominating regional areas or challenging the traditional approach to areas such as telecommunications, transport, and broadcasting. The best approach to regulation of the app-economy will reflect the complexity of the issues highlighted in these case summaries, with the aim to minimise disruption to the market without impacting the app-economy's growth and the immense value that it provides to society.

APPENDIX C:

OECD BASE EROSION AND PROFIT SHARING ('BEPS') REFORMS

A.1 Introduction

The 2015 Organisation for Economic Co-operation and Development (OECD)/G20¹²¹ Base Erosion and Profit Sharing ('BEPS') policy package seeks to close the gaps in international tax rules which allow Multinational Nation Enterprises ("MNEs") to artificially shift profits and avoid paying taxes. Enterprises operating in the digital economy, particularly OTT content providers, are noted as unique business models that enable global profit - splitting and -shifting.

The 2015 OECD report concludes that broad reforms are sufficient to address general BEPS issues in the digital economy. The project also identifies possible technical options to deal with further specific tax issues created by digital economy enterprises. However none are formally adopted as internationally-agreed standards. As the project shifts into an implementation and monitoring phase in 2016, these options may be adopted formally in the future.

A.2 Background

Globalisation has created opportunities for MNEs to reduce the taxes they pay through BEPS. BEPS refers to legal strategies that exploit the gaps and discrepancies between national tax regimes. BEPS arrangements allow profits to be shifted to low or no-tax locations.

The OECD estimates that between 4-10% of global revenue from corporate income tax is lost through BEPS by MNEs.¹²² Existing international tax instruments have not kept up with global economic developments, to the detriment of domestic market competition and taxpayers.

¹²¹ https://en.wikipedia.org/wiki/G-20_major_economies

¹²² OECD, 2015, 'Information brief: summary', see www.oecd.org/ctp/policy-brief-beps-2015.pdf

A.3 The Project

The OECD/G20 BEPS Project commenced in 2013. Member states agreed upon the need for multilateral efforts to improve international tax rules in response to the uniquely global problem created by BEPS. The project sought to develop mechanisms to ensure that MNEs report profits where economic activities occur and where value is created. The overall aim of the BEPS package is to close the gaps in international tax rules that allow MNEs to artificially shift these profits.

The project is the product of broad international cooperation. It was carried out by OECD and non-OECD G20 countries on equal footing. Extensive consultation was also undertaken with stakeholders, developing nations, and regional tax authorities.

A.4 Final recommendations

The OECD's BEPS project delivered its final recommendations in October 2015. The final BEPS measures include 15 central actions for nation-states to implement. Central arms of policy and reform include:¹²³

1. Reinforcing transfer pricing rules. The OECD Transfer Pricing Guidelines have upgraded the 'arm's length principle' to ensure what dictates results is an economic rather than paper reality (Actions 8-10). The requirements for transfer pricing documentation have also been substantially increased. This effort seeks to promote greater transparency around MNE operations (12, 13).
2. Strengthened tax treaty provisions. Changes to the Model Tax Convention have been agreed upon to ensure treaties are not used complex BEPS efforts. Treaty benefits will only be granted to those entitled to them (6). The definition of Permanent Establishment has also been modified to better reflect today's business reality (7).
3. Reforming domestic regimes. The report recommends that domestic governments eliminate preferential regimes that attract paper income over substantial business activities (5).
4. Bridging gaps among domestic laws. The report includes model rules and provisions to tackle hybrid mismatch arrangements, through more effective controlled foreign corporation rules ("CFC") in countries where headquarters are located (2-3).

In sum, the reforms aim to improve coherence, tighten the substance, and ensure more transparency in international taxation.

¹²³ OECD, 2015, *Executive Summaries*, see www.oecd.org/ctp/beps-reports-2015-executive-summaries.pdf

A.5 Digital economy-specific recommendations

The digital economy accelerates and changes the spread of global value chains in which MNEs integrate their worldwide operations.¹²⁴ Some of the features of the digital economy exacerbate BEPS risks. Digital economy MNEs also present further specific taxation challenges. As noted by the report, often it is difficult to capture digital economy enterprises within existing value-added tax collection mechanisms. This includes global OTT providers with businesses based on cross-border transactions.¹²⁵

During the consultation process, targeted policy measures were considered to meet these specific challenges. These include:

- A new nexus requirement, in the form of a ‘significant economy presence’;
- A withholding tax on certain types of digital transactions; and
- An equalisation levy.

The final report however, recommended that the broad BEPS actions would address BEPS issues exacerbated by the digital economy. In particular the ones on Permanent Establishment (“PE”), transfer pricing and controlled foreign company (“CFC”) rules were developed with digital economy business models in mind.¹²⁶ No digital economy-specific reforms were adopted as an internationally-agreed standard.

As the project shifts into an implementation phase in 2016, businesses will have to meet these stricter regulatory requirements. As implementation is evaluated, further reforms may be adopted for the digital economy space. Additionally, the report recommends that national governments monitor markets, and adopt any of the 3 options above as additional safeguards, as required.

¹²⁴ OECD, 2015, ‘Action 1 – Addressing the Tax Challenges of the Digital Economy’, Final Report, see www.keepeek.com/Digital-Asset-Management/oecd/taxation/addressing-the-tax-challenges-of-the-digital-economy-action-1-2015-final-report_9789264241046-en#page1

¹²⁵ OECD, 2015, ‘Action 1 – Addressing the Tax Challenges of the Digital Economy’, Executive Summary, see www.oecd.org/ctp/beps-reports-2015-executive-summaries.pdf

¹²⁶ OECD, 2015, ‘Policy brief’, see www.oecd.org/ctp/beps-reports-2015-information-brief.pdf

9 APPENDIX D: COMPANY CASE STUDIES

B.1 Introduction

In this section, case studies of selected global market leaders, regional market leaders and market disruptors will be elaborated on from Chapter 8. This section provides detail on the companies' history, services, structure and revenue of Airbnb, Alibaba, Apple, Facebook, Flipkart, Google, iSignthis, LINE, Netflix, Skype, SocietyOne, Tencent, and Uber.

B.2 Airbnb



Founded in 2008 and also headquartered in California, Airbnb operates as a market platform for users to list, find and rent lodgings, primarily on a short-term basis. Airbnb is not publicly traded, however its valuation as of its last funding round was USD24-25 billion, although aggressive growth assumptions underpin this figure 127. This makes it more valuable than the Marriott and Starwood hotel chains, and only slightly behind the Hilton group. Airbnb does not currently generate profit, although its revenue forecast for this year is approximately USD900 million. The lack of profit is caused by intense spending in order to secure continued growth in listings, footprint and bookings and is expected to change.

Airbnb operates as a market in which properly verified property occupiers can list their property, or part of it, as being available for guests to rent. Rentals can range from one night to more than a month and are at the discretion of the person listing the property. Prospective guests must also be properly verified in order to use the service, including providing a scan of a government-issued ID.

The service operates by having those looking for accommodation apply for listed properties, with the owner or head-lessor of the property then able to approve, or deny, the application. Airbnb generates revenue by collecting 6-12% of the price of the booking from the person seeking accommodation depending on the value of it and an additional 3% payment processing fee from the amount received by the person listing the property. As of May 2015 Airbnb has over 1.4 million properties available for tenants, from single rooms in apartments to private islands and more esoteric options such as windmills. In principle, any property can be listed for rental if the person listing it is properly verified.

¹²⁷ www.wsj.com/articles/the-secret-math-of-airbnbs-24-billion-valuation-1434568517

Like Uber, Airbnb has faced regulatory and legal headwinds in some cases. Cities such as New York, Santa Monica, Berlin and Tokyo have either proposed or put in place regulatory restrictions on short-term rentals. Common among these are minimum rental periods of 7, 28 or 30 days in specified areas or for specified types of dwellings. Airbnb has an average rental period of 5.5 days so the majority of its bookings would be prima facie illegal in these locations. A driving force behind these restrictions has been Airbnb not paying hotel taxes which other operators must pay, and the difficulty of regulating the standard of accommodation that is provided. At least one municipality has stated that it would be impossible to properly inspect and verify all the properties listed on Airbnb within its jurisdiction. While successful it is not without controversy, there have been reports of entire buildings being leased by a single person and then sub-leased via Airbnb for a profit.

Nevertheless, like Uber, Airbnb has had some success in having these regulatory barriers lessened or removed. It has done so in several ways. Firstly by demonstrating the value of its rentals to local economies, potentially millions of dollars per year. Secondly, by demonstrating positive social impacts, such as allowing low-income home-owners and renters to avoid foreclosure or eviction by sub-leasing parts of their properties. Finally, in many cases it has agreed to pay the relevant hotel taxes of the location a rental takes place in. Airbnb also supports a growing industry in property management, with companies that specialise in managing Airbnb listings on behalf of the owner or head-lessor now operating in several jurisdictions.

Despite some initial regulatory headwinds Airbnb appears likely to continue growing as a major disruptor to the existing hospitality industry, in particular traditional hotel operators with many already seeing the impact of competition from Airbnb listed properties.

B.3 Alibaba



Alibaba is a Chinese e-commerce company which provides consumer-to-consumer, business-to-consumer and business-to-business sales services via different web portals. Since its founding in 1999 it has also expanded to provide ePayment services, a shopping search engine and commercial cloud-computing services. Alibaba was initially founded a business-to-business sales portal which was used to connect Chinese manufacturers directly to international customers.

Alibaba operates Taobao, a consumer-to-consumer portal similar to eBay which has a catalogue of over 1 billion products and is one of the world's most visited websites. Alibaba group websites account for more than 60% of parcels delivered in China and more than 80% of China's online sales. Its annual 'Singles' Day' shopping event generated sales of USD14.32 billion in 24 hours on November 11 2015.

In September 2014 Alibaba listed on the New York Stock Exchange raising USD25 billion and giving a market capitalisation of more than USD250 billion. This was the largest IPO in US history and one of the largest in global history. Since listing its shares have declined in value, but its market capitalisation is still over USD200 billion.¹²⁸

In addition to the subsidiaries created organically such as Taobao and Alipay, Alibaba Group has purchased stakes in companies such as Weibo and Lyft and was a stakeholder in Kuaidi Dache prior to its merger with Didi Dache.

Taobao is Alibaba's major platform and functions as a consumer-to-consumer online shopping portal similar to eBay. It has achieved massive popularity by offering commission free transactions using a third-party payment platform. In lieu of generating revenue by taking commissions it does so by charging for advertising on the platform. Its annual sales exceeded 1 trillion Yuan (USD160 billion) in 2012 and have continued growing since.

Alipay is a third-party online payment platform launched in 2004. It charges no transaction fees and also provides escrow services to buyers and sellers. Alipay was spun off by Alibaba Group in 2010 and now accounts for more than half of China's online payment market.

As part of its tenth anniversary in 2009 Alibaba launched a commercial cloud computing service called Aliyun which includes e-commerce, data processing, data mining and data customization services. It has R&D centers in Hangzhou, Beijing and Silicon Valley and is the largest provider of high-end cloud computing services in China. In 2014 Alibaba acquired a controlling stake in ChinaVision Mediatv which was subsequently renamed Alibaba Pictures. As of 2015 it is the largest Chinese film company by value.

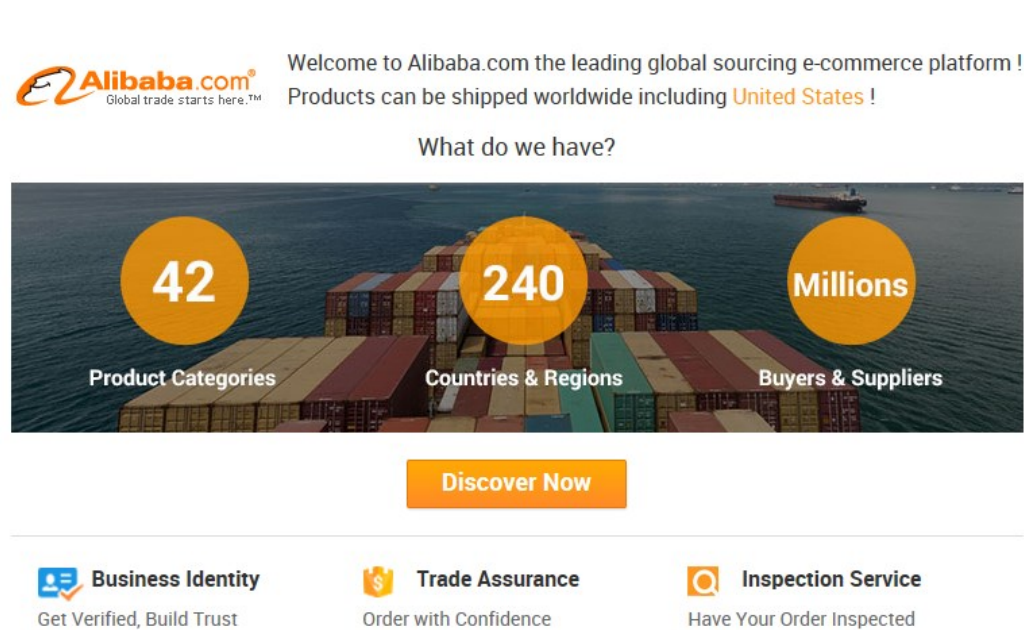
Alibaba has become one of the largest companies globally and in particular in its home market of China by breaking from the usual business models of similar companies. Its largest services operate at no or low cost to users and instead generate revenue from third parties. This has allowed Alibaba to process extreme volumes of transactions, representing dominant market share within China.¹²⁹ By monetizing the popularity of its services, rather than the services themselves, Alibaba has managed to continue achieving major growth in users both among consumers and the businesses using its services.

Like many companies which reach such a size it has now diversified away from its core of e-commerce and expanded beyond its home market of China. While there have been fluctuations in its share price, and consequently market capitalisation, it has regained its place as one of China's most valuable companies as of December 2015.

¹²⁸ Source: NYSE 22 December 2015.

¹²⁹ <http://qz.com/501241/alibabas-stock-price-is-taking-a-beating-but-that-doesnt-mean-alibaba-will-too/>

Figure 40: Alibaba home page



Source: Alibaba, 2016

B.4 Apple



Founded in 1976 and with its headquarters in California, Apple is the world's largest information technology company that designs, develops and sells consumer electronics, computer software and online services. Soon after the release of the iPhone in 2007, Apple launched the first App Store with 552 apps.

The App Store is a digital distribution platform for mobile apps on iOS, a mobile operating system created and developed by Apple and distributed exclusively for Apple hardware. The service allows users to browse and download applications that are developed with Apple's iOS software development kit (SDK). Apple takes 30 percent of all revenue generated through apps, with 70 percent going to the app's publisher. The apps can be downloaded directly to iOS devices such as the iPhone smartphone, the iPod Touch handheld computer and the iPad Tablet computer, or onto a personal computer via iTunes.

From its launch in 2008, the App Store has seen exponential growth both in revenue generated and apps created. Within one month after its release, the number of apps downloaded reached 60 million, with the top 10 developers earning USD 9 million. In the past seven years, Apple has paid almost USD 40 billion to app developers, 33% of which was generated in 2015. It is estimated that the App Store generated approximately USD 6 billion in operating profit for Apple in 2015, which would make up close to half of the company's total operating profit growth in that year. The iTunes Store, which contains the App Store, is the only line from Apple's vast array of services and products that has been consistently growing above 10 percent in revenue for the past 8 years. It is therefore predicted that the App Store will be a significant growth driver of operating income in oncoming years for the company.

Alongside contributing to Apple's growth in revenue, nearly three-quarters of the 1.9 million jobs created by Apple in the U.S. are attributable to the community of app creators, software engineers and entrepreneurs building apps for iOS, as well as non-IT jobs supported directly and indirectly through the app economy.¹³⁰ The iOS app economy has additionally created 1.2 million jobs in Europe and 1.4 million jobs in China.

The strongest markets for Apple's iOS are the U.S, Japan, Canada and Western Europe, which show proportionally higher ratios of developers using the iOS platform. Although Apple envisions the App Store to be a global product, in reality its market is restricted to national boundaries, a division that helps to ensure that the associated commerce abides by all country-specific content policies and tax laws. Thus, there are potentially as many distinct App Stores as are countries in the world.

B.5 Facebook



Facebook was launched in 2004 and is headquartered in California, USA. It has a market capitalisation of approximately USD294 billion and had revenue of USD12.44 billion in 2014.¹³¹ It has over 12,000 employees based primarily at four major sites in California, Hyderabad, Dublin and Texas, along with several data centres globally. Facebook is the world's most ubiquitous social network with more than one billion active users daily, including more than 1.4 billion mobile users monthly. Facebook's primary source of revenue is advertising with an emphasis on being able to target advertising to specific users and groups of users. It is noteworthy that mobile users accounting for approximately 60% of generate approximately 78% of advertising revenue.¹³² Revenue and profitability has grown year on year, at least partially driven by increased investment in advertising technologies and user experience.

¹³⁰ Job creation estimate based on research by Dr. Michael Mandel, Progressive Policy Institute. "App Economy Jobs in the United States," January 6, 2016

¹³¹ Source: NASDAQ, December 22 2015.

¹³² www.nytimes.com/2015/11/05/technology/facebook-q3-earnings.html?_r=0

Facebook is primarily a social networking platform which leverages its ubiquity and its wealth of user data to generate revenue through advertising on its site. Currently the majority of this is advertising in side bars and banner ads, however it has expanded into video advertising and shown significant growth in this area. Facebook has also worked directly with some advertisers in order to create more bespoke or widespread advertising campaigns than its standard products.

In recent years, it has joined other major technology companies as an acquirer of start-ups which it believes align with its business model or which have significant long term potential. Currently, Facebook is the head company of photo social network Instagram, messaging app WhatsApp and virtual reality headset manufacturer Oculus VR.

Currently, Facebook has not monetized any of its subsidiaries, and analysts believe that there may be potential upside for Facebook's revenue figures in future if it does decide to do so. It has recently commenced including advertising in the Instagram platform, although as yet neither WhatsApp nor Oculus VR generate any revenue. A focus on the long-term value of these acquisitions has been costly in the short term but is likely to pay off in the longer term if they are monetized sustainably as a result. There would be little point generating short-term ad revenue from WhatsApp if the result was customers abandoning the service.

The majority of Facebook's revenue comes from advertising on its mobile app, which also accounts for a significant number of its users. In addition, two of its major subsidiaries are app-based services (Instagram and WhatsApp), while only one is hardware based (Oculus VR). It also supports a secondary industry in game and app development for use within the Facebook website and mobile app (see, for example, Farmville).

Facebook is not a disruptor in the sense that it is causing a restructure of an established industry, however its total ubiquity as a social network, to the point that it largely does not have any direct competition, makes it a key player in the app economy. The major thing holding Facebook back is its having been outlawed in some countries (for example China) and local preference for home-grown social networks in others (for example Russia). In future Facebook may face competition from local competitors in significant markets such as Weibo in China as take up rates there increase. However, continued investment in new technologies and subsidiaries which have the potential to augment its future revenue leaves it in a strong position. Facebook has been willing to takeover start-ups with significant potential upside even outside its core of advertising, so it is likely to diversify over time if these subsidiaries grow and become profitable.

B.6 Flipkart



Flipkart is India's biggest electronic commerce company, established in 2007 by two former Amazon employees. Headquartered in Bangalore, Flipkart's services are exclusively available to India.

The company began by selling books and soon expanded to a wide variety of goods. Flipkart has since launched its own product range under the name 'DigiFlip', with goods including tablets, USBs and laptop bags. Flipkart has also launched 'Flyte', a paid music download service.

Flipkart first raised funds through venture capital funding. As the company grew in stature, more funding arrived. In the financial year 2009-09, Flipkart had made sales of approximately USD600,000. This soon increased to just under USD3 million the following year. As of May 2015, the company's valuation is at USD15.5 billion.¹³³ In addition, Flipkart has acquired other e-commerce websites such as Myntra.com and LetsBuy.com to better their presence in the Indian market.

Until 2013, Flipkart sold goods directly to consumers. Flipkart has since turned to a marketplace model, allowing third party businesses to list their products and sell on their platform. The company offers stocking and shipping service to the merchants selling their products on Flipkart, a service called 'Flipkart Advantage.' The merchants stock their products at Flipkart's warehouses before the orders are placed, with Flipkart informing the merchants of the quantity of products based on intelligence gathered from the history of demand for that product. As products are available with Flipkart at the time the order is placed, quality checks and expedited shipping is possible.¹³⁴ Customers of Flipkart consequently receive 30-Day hassle-free returns on products as well as expedited delivery options such as Same-Day Guarantee Delivery.¹³⁵

Flipkart also pioneered cash on delivery and payment by card on delivery services to its consumers, an option in which most online shopping websites in India offer today.

Two-thirds of Flipkart's 8 million monthly shipments come from cities and small towns, where most people do not have access to desktop computers and broadband Internet. This means that smartphones are the primary platform for e-commerce in India, with the country being the third largest market for smartphones in the world. Acknowledging these trends, Flipkart plans to shutdown its website in 2016 and transition completely to a mobile app to deliver its services.

¹³³ www.wsj.com/articles/flipkart-valued-at-15-billion-after-latest-funding-1432088548

¹³⁴ <http://trak.in/tags/business/2014/09/18/flipkart-advantage-stocking-shipping-service/>

¹³⁵ *ibid.*

B.7 Google



Google Inc. is an American multinational technology company specialising in Internet-related services and products. Google entered the smartphone industry in 2005 through the acquisition of Android Inc. The Android platform is a fully integrated mobile 'software stack' that consists of an operating system, middleware, user-friendly interface and applications. It is the first open and comprehensive platform for mobile devices, made available under open-source licences that give mobile operators and device manufacturers flexibility in designing their own products.

Google Play, which was originally born under the name Android Market in 2008, is Google's official store and portal for Android apps, games and other content for Android powered phones, tablets or Android TV devices. It allows users to browse and download applications developed with the Android SDK and published through Google. Apps are available through Google Play either free of charge or at a cost. They can be downloaded directly to an Android or Google TV device through the Play Store mobile app or by deploying the application to a device from the Google Play website. Google, like Apple's App Store, keeps 30% of revenue from the apps sold on Google Play, with the remaining revenue passed onto the publisher.

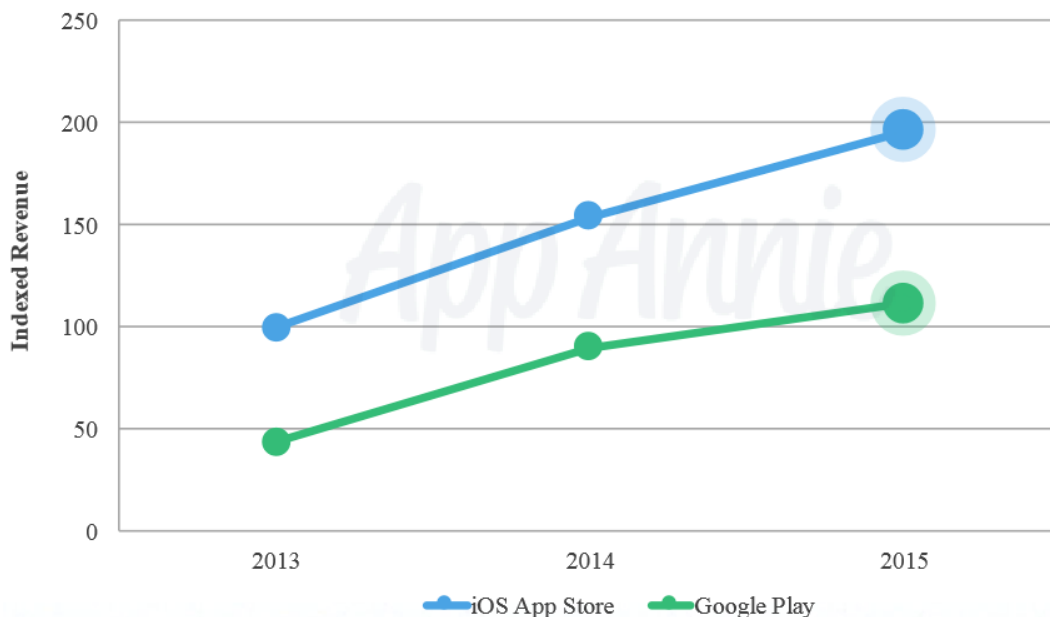
Google launched the Android Market in 2008 with only a handful of apps. By May 2012, the number of available apps in the Google Play Store surpassed 1 million, and was placed at 1.8 million apps in November 2015. In the third quarter of 2015, Google Play had 100% more app downloads than Apple's App Store, a figure largely attributable to bolstered demand in emerging markets such as India, Brazil and Indonesia alongside the globally dominant use of Android smartphones by end-users and developers. Despite these numbers, Apple's App Store continues to generate approximately 80% more revenue than Google Play for developers. This trend is exhibited in the graph below.

Two reasons have contributed to this revenue between the App Store and Google Play. Primarily, as Apple handsets are more expensive, it is hypothesised that their more affluent owners are prepared to spend more money on apps than the 'average' Android user.¹³⁶ Furthermore, Google has removed a majority of its services in the Chinese market after the company refused to continue self-censoring its search results in 2010. This means that the Google Play store gains no revenue from the Chinese market, whereas the Apple App Store does. However, Google has announced its plans to launch the Chinese version of its Google Play smartphone app store in 2016, presumably in an attempt to fill this gap in revenue.¹³⁷

¹³⁶ www.androidauthority.com/google-play-store-vs-the-apple-app-store-601836/

¹³⁷ www.reuters.com/article/us-alphabet-china-idUSKCN0T91K420151120

Figure 41 Annual worldwide App revenue (millions USD)



Source: App Annie

B.8 iSignthis



iSignthis Limited (ASX: ISX) is based in Melbourne, Australia with a European presence in Amsterdam and Cyprus, the United Kingdom and representatives in the US and Asia.¹³⁸ Founded in 2013, its initial focus was preventing Card Not Present (CNP) fraud in order to protect consumers and merchants from the growing problem of online fraud.

iSignthis is now a global leader in online, dynamic verification of identity and financial transactions via regulated e-payment instrument authentication. The automated, online identification of persons remote to the transaction is made possible via a patented electronic verification method, and is available to more than 3.5 billion financially included persons, no matter where they are located. iSignthis also assists merchants with CNP liability shift, within the framework of the card scheme rules and applicable regulatory regimes. . ISX was the best performing small cap on the ASX in 2015.

iSignthis provides the legal basis for compliance to meet customer identification requirements for anti-money laundering (AML) obligated entities, as well as operational benefits for any online business looking to reducing customer on-boarding friction, mitigating CNP fraud, monitoring transactions and streamlining operations. It has a number of patents and patents pending in this area.

¹³⁸ One of the authors of this report, Scott Minehane is currently a non-Executive Director of iSignthis Limited.

B.9 LINE



Line is a proprietary application for instant communication on smartphones, tablets and personal computers. It enables the instant exchange of texts, images and videos as well as free VoIP voice and video calls between users. It was designed and is owned by a subsidiary of Korean internet search company Naver.

LINE was first launched in Japan in 2011 and reached 100 million users within 18 months and 200 million users within 2 years of its initial launch. LINE became Japan's largest social network in 2013 and passed 600 million worldwide users by February 2015. It is expected to have surpassed 700 million total global users by the end of 2015. Originally released on Android and iOS, LINE is now also available for BlackBerry, Nokia Asha, Windows Phone, Firefox OS, iOS tablets and as a Google Chrome browser application.

LINE was initially developed as an internal communications system for NHN Japan employees in the wake of the 2011 Tohoku earthquake, which severely damaged telecommunications infrastructure and left the company reliant on internet-based communications while the infrastructure was restored. After its development NHN decided to release LINE to the public and explosive growth immediately followed. As a result of this success a dedicated subsidiary Line Corporation was set up to manage LINE and related products.

Initially only a messaging service, LINE has developed in the direction of a social network, with users now able to make use of bulletin boards, timelines and homepages on which they can post, upload pictures, and like and comment on other people's posts and uploads. LINE allows users to purchase 'stickers' in an online store, which act as super-sized emojis that can be sent in messages and used in chat sessions between users. More than 1 billion of these stickers are sent daily by LINE's users worldwide.

For users in China LINE conforms with government-imposed censorship requirements which prevent discussion of topics such as Tiananmen Square and controversial discussion of Tibet and Hong Kong.

While it is used globally, LINE has particular significance in some specific markets. In particular, it is the dominant messaging and social network service in Japan and Thailand with 50 million and 22 million users respectively, and is a significant market force in Indonesia, Taiwan, Spain and India with 16 million or more users in each.

In addition to its instant-messaging function LINE also has a significant cultural impact, particularly in Japan, with television shows based around it produced in recent years. Its ubiquity has also led to it being depicted in international television shows and music videos as the messaging service used by characters in the show.

In 2015 LINE launched a taxi service in Tokyo, intended as a competitor to Uber. It also launched an app which allows for group calls of up to 200 participants in June 2015. It also recently enabled the use of end-to-end encryption for one-to-one messaging on its

platform where both parties to the conversation have the appropriate option enabled in their LINE app.

LINE's revenue for 2015 is expected to exceed USD800 million, while this represents significant growth on that in 2014 it appears to have stagnated with little growth in revenue between quarters in 2015.¹³⁹ LINE remains dominant in Japan, Thailand and Taiwan but has not seen the same rapid uptake in other markets that it initially did in these core three. LINE has addressed this issue by releasing new services such as an iOS keyboard app and a 'lite' version of its app for emerging markets.

B.10 Netflix

NETFLIX

Netflix was founded in 1997 as an online DVD rental service using the traditional model of a per-rental fee. Since then it has morphed into a monthly-subscription based video-on-demand provider which produces its own content and is responsible for approximately 30% of all internet traffic in some of the countries where it operates.

This transformation has been gradual. In 1999 Netflix began offering a monthly-subscription service for DVD rentals, with different tiers of membership allowing different numbers of DVDs per month. In 2000 it stopped offering per-rental services and became solely monthly-subscription based. In 2007 Netflix offered its initial video-on-demand service free of charge to monthly-subscribers, with viewing limits based on the DVD rental subscription tier they held. Due to increasing demand for streaming, Netflix began offering streaming-only subscriptions to customers in November 2010. Its current model is based on streaming subscriptions with an optional surcharge to also gain access to DVD or Blu-Ray rentals.

Beginning with Canada in 2010, then Latin America, Europe, and Australia, Netflix has progressively expanded its global footprint. As of January 2016, Netflix can be accessed in 130 countries including Vietnam, Indonesia, Saudi Arabia and Russia, with China standing as the only major country that does not have access to the media-streaming service.

Netflix now has approximately 74 million subscribers worldwide, of which about half are in the US. Considering its recent global expansion in 2016, it is probable that these numbers will substantially increase. The total number of users is likely to be significantly higher than the subscription figure listed as a single subscription allows up to four profiles to be created, and each profile may be viewed by multiple people simultaneously, much as one television serves an entire family. Netflix had revenues of approximately USD 6.1 billion in

¹³⁹ <http://techcrunch.com/2015/07/29/chat-app-lines-revenue-falls-for-first-time-amid-struggle-for-global-growth/>

2015¹⁴⁰ and currently has a market capitalisation of almost USD 50 billion.¹⁴¹ Netflix is headquartered in California and currently has over 2,400 employees.

¹⁴⁰ http://files.shareholder.com/downloads/NFLX/1305047504x0x854558/9B28F30F-BF2F-4C5D-AAFF-AA9AA8F4779D/FINAL_Q3_15_Letter_to_Shareholders_With_Tables_.pdf

¹⁴¹ Source: NASDAQ 22 December 2015

Beginning in 2011 Netflix is now a producer of its own content, not solely a provider of access to content owned and produced by other parties. The airing of House of Cards in 2013 marked the beginning of the availability of Netflix's self-produced content. This content is a mix of original movies and television shows, and some cases where Netflix has secured the rights to produce new series of existing shows after they have been dropped by their original producer.

Netflix is credited with bringing about significant change in consumer preferences and in the way consumers watch video content. Its streaming service allows users to 'binge' watch programming, without being locked into the nightly or weekly airing schedule of traditional programming. This has in turn allowed a shift in the way television shows are produced, with no need for cliffhanger endings which entice viewers to return the following week. It has also allowed a break with traditional requirements of fitting content into 30 or 60 minute windows with space for advertising built in.

Netflix has also become involved in the debate surrounding net neutrality, largely as a result of the amount of bandwidth used on its streaming services. Currently Netflix pays some ISPs in order to ensure its customers have sufficient bandwidth and usage caps to use its services. Netflix would be a major beneficiary of any net neutrality legislation.

B.11 Skype



Initially launched in 2003 Skype is a VoIP, video chat, and instant messaging platform which is available on Windows, Mac, Linux, Android, Blackberry, iOS and Windows Phone operating systems, as well as associated tablets. Skype was created by Swedish and Danish developers with assistance from Estonian programmers and initially shared its backend systems with the music sharing application Kazaa.

In September 2005 eBay acquired Skype from its original owners for USD2.6 billion. In 2009 65% of Skype was acquired for USD1.9 billion. This acquisition was made by a combination of investors including the Canada Pension Plan Investment Board. In 2011 Microsoft acquired Skype for USD8.5 billion and incorporated it as Skype Technologies, a wholly owned subsidiary. The Skype division of Microsoft is headquartered in Luxembourg, but a substantial proportion of its development team and employees are based in Estonia.

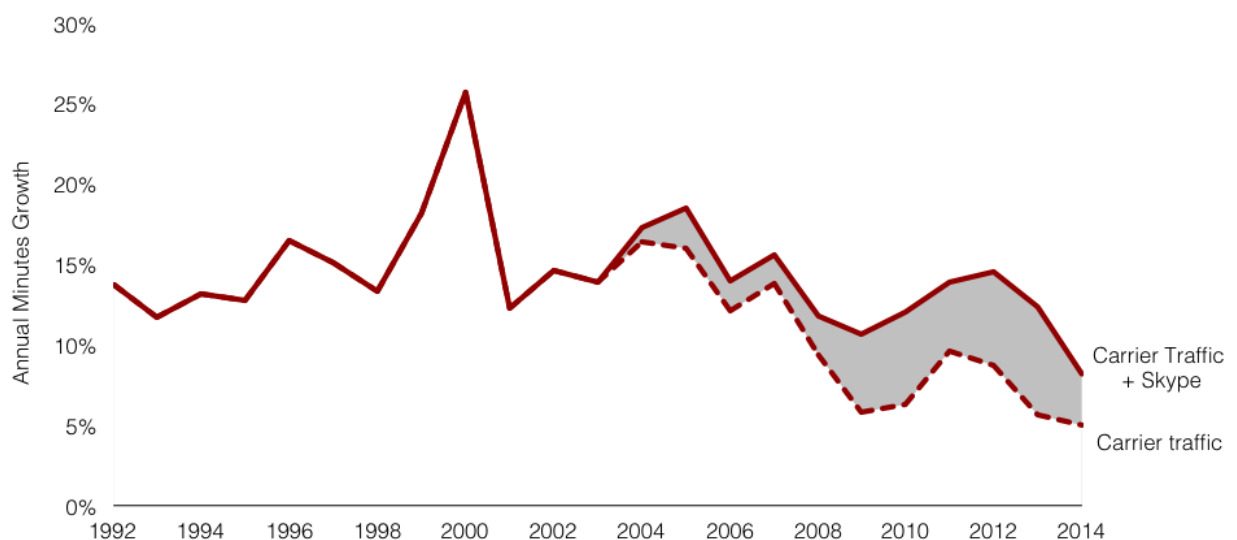
Skype operates using a freemium model in which Skype-to-Skype calls are free for both caller and receiver, while calls to landline or mobile phones are charged via a debit-based system. In some cases network administrators have banned the use of Skype on corporate, government or education networks for reasons such as inappropriate use of network resources, excessive bandwidth usage, particularly for video calling, and security concerns.

Since its acquisition by Microsoft Skype is powered by Microsoft proprietary infrastructure, in contrast to its beginnings as a peer-to-peer/client-server system hybrid. Microsoft has continued the development of existing Skype services as well as incorporating Skype technology into its own offerings. For example, as of 2013 Skype has replaced Microsoft's Windows Live Messenger globally except for China.

Skype provides each user with a unique Skype name which can be stored in a Skype Directory and which users can use to add each other to address books. Skype allows one-to-one voice and video calling using a proprietary codec as well as voice and video conference calling between up to 25 users, all of which is free between Skype users. Skype also provides a service which allows users to receive calls on their computers which originate on conventional telephony networks. It does so by providing a local number which is linked to the users Skype name. This service is available in specific countries only, although the number where it is available is significant.

As of 2014 it is estimated that Skype accounts for 40% of all international calling with continued growth in total minutes from the 214 billion recorded for 2013.¹⁴² This is likely attributable to its freemium model whereby users with any computer, tablet or smartphone can communicate with any other user with a similar device, for free using the Skype app.

Figure 42: The Skype effect on international voice growth rates



Source: Telegeography 2014

Skype is not directly available in China, however a localized version is available.

¹⁴² www.telegeography.com/products/commsupdate/articles/2014/01/15/skype-traffic-continues-to-thrive/

Skype has been widely used for educational purposes, including pairing native speakers of different languages with each other to facilitate conversations which alternate between each language in order to promote learning. Skype is also used to provide eLearning programs, whereby conference calls allow a teacher to communicate with students spread across different geographical areas, including remote areas, at the same time.

Skype has significantly disrupted traditional telephony, and in particular conference calling, however it is unclear what percentage of its total minutes of use are free Skype-to-Skype calls and how many are paid Skype-to-traditional network calls.

B.12 SocietyOne



SocietyOne is one of a number of 'peer-to-peer' lenders which launched in Australia in August 2012. It facilitated loans worth AUD1 million by January 2013, AUD 4 million by March 2014 and AUD30 million by May 2015. While described as 'peer-to-peer' lending, the majority of SocietyOne's capital comes from institutional investors such as Westpac and News Corporation, and it is not yet open to retail investors.

Australian financial services disclosure requirements mean that it has restricted its ability to invest in loans to institutional, professional and sophisticated investors only, although retail investment offerings are planned. This has led to SocietyOne being termed a 'marketplace lender' rather than a true peer-to-peer lending platform.

SocietyOne operates as a platform on which borrowers can list their profile, including loan term, loan purpose, and financial information. Once they have done so lenders can bid to fund their loan in a reverse auction of the interest rate they are prepared to accept for lending to the borrower. In effect, SocietyOne provides a technology platform which matches borrowers with investors, ideally offering both a better interest rate than they would receive from traditional financial institutions.

SocietyOne has grown rapidly, as its loan origination figures indicate, however it still only accounts for a tiny percentage of the Australian consumer credit market. Since its launch SocietyOne has expanded its offering from exclusively unsecured consumer credit (personal loans), and now offers livestock loans as well. Money invested by lenders in SocietyOne is held in a bankruptcy-remote trust vehicle and cannot be used to pay debts or obligations of SocietyOne as an entity. SocietyOne's approval rate for loan applications is approximately 15%, and from inception to 2014 its default rate was 2.3%. This approval rate is around half of that of larger financial institutions for first-time borrowers and is deliberate in order to ensure that early-stage investors have positive results for their investment. By ensuring early success for investors SocietyOne should be able to secure increased investor interest in future, without which expansion will be impossible.

SocietyOne matches lenders and borrowers using proprietary technology developed by one of its co-founders and tested using traditional banking services. SocietyOne's revenue is approximately 5 percent of the loans originated comprised mainly of a 1.25% management fee paid by the investor and an origination fee paid by the borrower once a loan is originated, which averages 3.5%. Late payment fees are similar to major Australian banks and there are no servicing or prepayment fees.

SocietyOne's main competitor in Australia is Ratesetter, which launched in November 2014 and is part of the Ratesetter group, based in the UK and founded in 2010. ThinCats Australia is an offshoot of ThinCats, which is also based in the UK, and which specialises in peer-to-peer funded small business loans. MoneyPlace is a newer market entrant which was founded by a small group of executives from one of Australia's four major traditional banks. Its investment model involves fractionalising loans as a means of diversification and risk minimisation for investors. Finally, OnDeck is a New York based small business lender which announced a partnership with Australian listed accounting software provider MYOB commencing in December 2015. While still nascent, the Australian P2P lending market is predicted to reach AUD10.4 billion, or 6 percent of total consumer lending by 2020, while the global P2P lending market could grow to between USD150 and USD490 billion by 2020.¹⁴³

B.13 Tencent

Tencent 腾讯

Tencent is a conglomerate headquartered in Shenzhen, China which as of September 2015 was the largest internet company in Asia by market capitalisation. It was founded in 1997 and its initial success came from owning and operating the QQ instant messaging service. Tencent listed on the Hong Kong Stock Exchange in 2004 and was added to the Hang Seng index in 2008. After initially deriving revenue exclusively from advertising in and premium users of QQ Tencent has since expanded to become a major conglomerate, with subsidiaries and joint ventures including the JD.com e-commerce website, creation of online games, sale of virtual goods, media distribution, online auctions, taxi hailing, social media, online search and online payments.

Tencent is also the owner of the WeChat social mobile application, the most popular app in China. In 2011 Tencent acquired a majority interest in Riot Games, developer of the popular online battle game League of Legends. It also owns minority stakes in Epic Games, a major game production studio and Activision Blizzard, one of the world's largest video game production and publishing companies. These acquisitions increased its game creation portfolio beyond its domestically focussed, and to a lesser degree mobile focussed, origins.

¹⁴³ www.afr.com/business/banking-and-finance/societyones-30m-of-p2p-loans-the-tip-of-an-iceberg-20150522-gh7jca

Its original platform, Tencent QQ remains one of the largest instant messaging platforms globally, with peak simultaneous usage exceeding 100 million active users on more than one occasion. Combined with WeChat this makes Tencent one of, if not the largest, instant messaging service providers worldwide with more than 1 billion total users.

Tencent is also a major media distribution provider for the PRC, with exclusive Chinese distribution rights for Sony, Warner Music Group and YG Entertainment music, HBO television and for NBA basketball games in China.

Tencent is also a major operator in the taxi hailing market in China. In conjunction with Singapore's Temasek Holdings, Tencent led investment of USD700 million in ride-hailing app company Didi Dache. Similar to Uber, this app works by using gps-based location data to match customers and taxi drivers in an area. Didi Dache is dominant in the Chinese taxi-hailing industry, with market share of more than 60% and services extending to most major urban centres. Between 2013 and 2014 it doubled its registered consumer user base from 20 to 40 million. It processes more than 21 million cab rides each month and has a user base of more than 350,000 taxi vehicles and drivers. In early 2015 it was announced that Didi Dache would merge with its main rival Kuaidi Dache but continue to operate as a separate brand. Details of Tencent's holding in the merged entity are not publicly available.¹⁴⁴

Tencent has faced controversy, primarily on two fronts. It has been noted by some commentators that many of Tencent's products and services are similar to those already offered by competitors and several competitors have accused it of copying existing services and products. It has also faced challenges by anti-malware ranking websites, which have accused its software of being designed to game anti-malware testing so as to appear more benign than is actually the case.

Tencent currently has a market capitalisation of USD184 billion, and recently peaked at more than USD200 billion (note these figures are impacted by exchange rate fluctuations in addition to stock price movements).¹⁴⁵ Its 2014 revenue is listed as approximately USD12 billion and it has more than 27,000 employees worldwide.

More recently, Tencent has partnered with Apple and Twitter to provide enterprise cloud services, and with IBM to provide SaaS services. Another significant source of revenue is licensing of its iconic penguin character mascot.

B.14 Uber



Uber was founded in 2009 and is headquartered in San Francisco, California. Uber operates a mobile app which connects customers with smartphones to drivers using the corresponding app in order to provide them with transportation. Depending on the

¹⁴⁴ www.reuters.com/article/us-china-taxi-merger-idUSKBN0LI04420150214

¹⁴⁵ Source: Bloomberg, 22 December 2015

country, city and type of Uber service selected this can be in the form of registered limousine, ordinary private car, boat, air balloon or even helicopter.

Investors in Uber include Google Ventures, Tata, China Life Insurance Co, the Qatar Investment Authority and Baidu, which also provides Uber with mapping and traffic data in Chinese cities. Uber is valued at over USD 60 billion and its revenue is estimated at USD 2 billion for 2014, predicted to grow to over USD5 billion in 2015.¹⁴⁶ Uber does not currently make a profit, with its chief costs being marketing, driver incentives and the cost of legal and regulatory disputes and related lobbying efforts.

After a launching in San Francisco in February 2011 Uber has expanded rapidly and aggressively around the world, beginning with Paris in December 2011 following domestic US expansion. The Uber app currently allows customers to book rides in over 300 cities in more than 59 countries worldwide including most recently Nigeria, Kenya and Lithuania.

Uber generates revenue by collecting 20% of the fares earned by the drivers using its app. These fares are transferred between the customer and driver automatically using a credit card which must be registered with Uber in order for the customer to request a ride.

The vast majority of rides booked using Uber are for either registered limousines, or similar vehicles registered for commercial provision of transportation, driven by similarly accredited drivers, or for ordinary cars driven by drivers without professional accreditation. The latter service has proven to be significantly disruptive to the taxi industry and has been a major source of controversy. In many jurisdictions Uber's services, in particular those facilitating rides in vehicles without a commercial registration or taxi license, are against existing laws. Uber's business model has been to launch these services regardless and then use customer support as a platform for lobbying against the regulations which restrict its services. This strategy has been widely successful, with notable exceptions such as France, Spain and Thailand, which have banned its services outright.

A major source of controversy is the impact of these services on licensed taxi industries, which in many cases requires ownership of a taxi license, or medallion, which has significant capital value. These licenses are devalued by the introduction of competition from Uber, and some governments have authorised Uber on condition that it applies a surcharge to fares in order to compensate owners of taxi licenses which have lost their value.¹⁴⁷

Other sources of controversy include the safety of passengers using Uber services and the impact on the livelihood of taxi drivers and similar interest groups. There have been widespread protests and strikes by taxi drivers against Uber, with varying success.

Uber has partnered with finance companies who are prepared to lend to prospective drivers so they can purchase a vehicle and use their earnings from Uber to repay the loan. It has also run promotion in which Uber drivers deliver ice cream, or even kittens to

¹⁴⁶ www.reuters.com/article/us-uber-tech-fundraising-idUSKCN0QQQG320150821

¹⁴⁷ www.abc.net.au/news/2015-12-17/uber-x-legalised-in-nsw-under-government-proposals/7037600

customers to play with. Uber is succeeding in its push to be legalized where it faces regulatory hurdles, and its projected growth is unlikely to stop or slow down.

A final point of controversy for Uber has been taxation. Uber repatriates profits earned to its US home, which has been a controversial practice in some jurisdictions. It has also been involved in taxation disputes in inter alia Australia, regarding incorporating VAT and similar taxes into its fare prices. As of late 2015 it now includes GST in Australian fares.

GSR-16 Discussion Paper

MAINTAINING TRUST IN A DIGITAL CONNECTED SOCIETY

Work in progress, for discussion purposes

Comments are welcome!

Please send your comments on this paper at: gsr@itu.int by 30 May 2016



The views expressed in this paper are those of the author and do not necessarily reflect the opinions of ITU or its Membership.

This paper was prepared by Douwe Korff, Emeritus Professor of International Law, London Metropolitan University, Associate, Oxford Martin School, University of Oxford

CONTENTS

Executive Summary with recommendations

Part 1: The broad context: Data, trust and security in the digital world

- 1.1 Introduction
- 1.2 Consumer trust and technical security
- 1.3 Consumer trust and the regulatory framework

Part 2: Privacy, data protection, universality and free data flows

- 2.1 Global challenges; different concepts and approaches
- 2.2 Privacy and data protection
- 2.3 Universality of human rights
- 2.4 The regulation of global personal data flows in the main international data protection instruments and model laws
 - 2.4.1 The dilemma
 - 2.4.2 Non-binding guidelines
 - 2.4.3 Binding regional data protection instruments with international reach
 - 2.4.4 Model laws
 - 2.4.5 Jurisdiction
 - 2.4.6 Data protection: global convergence and cooperation

Part 3: National security, public security and cybersecurity, and trade agreements

Part 4: Roles and responsibilities of regulators

- 4.1 Different and overlapping frameworks
- 4.2 The emerging global data protection framework
- 4.3 Data protection regulators in practice
- 4.4 Other regulators

Notes

Executive Summary

1. The development of the global digital connected society requires trust and security, based on sound regulation of the use of personal data. However, this is hampered by conceptual differences between states as concerns privacy in a narrow sense and data protection in a broad sense, and by different views on the application of the basic norms to non-nationals and to people outside a state's territory (the issue of universality of human rights).
2. The answer can only be found in global acceptance of a broad human rights-based concept of data protection that states must apply to "everyone" affected by their actions, irrespective of nationality or legal status or the place where they live. The global digital connected society can only develop in and between states that accept this fundamental principle.
3. There is the beginning of global convergence in terms of the contents of and approaches in data protection laws, with a trend towards adoption of laws on the "European" lines, and the establishment of special, independent and adequately resourced privacy- or data commissioners with strong investigative and enforcement powers, as demonstrated by the "Model Laws" drafted with support of the ITU and the EU for the Caribbean, Central and Sub-Saharan Africa.
4. There is strong global support for closer and more effective cross-border cooperation, not least as concerns the development of rules and tools to allow international data transfers – *either* because they occur between countries that have effectively the same levels of protection, *or* because "appropriate safeguards" are provided by various means and mechanisms such as data transfer contracts, Binding Corporate Rules, sectoral Codes of Conduct, or privacy seals.
5. The "modernised" Council of Europe Data Protection Convention, which is open to all states (not just to European ones) can become a global reference for data protection on which mutual assistance and mutual recognitions can be built if (as intended) the revised Convention, like the "Model Laws", will be aligned with the new EU data protection rules. The Convention and the Model Laws can in this way between them become a bridge between the EU, the Council of Europe Member States, and the rest of the world in terms of free data flows.

However, there are also obstacles:

6. First of all, there are jurisdictional challenges in relation to:
 - the duty of states to ensure data protection to anyone "within their jurisdiction" (see points 1 and 2, above);
 - the application of national data protection laws extraterritorially to activities by people or companies – or even public bodies – in other states; and
 - the increasingly common cross-border "pulling" of personal data by one state's agencies from servers or devices that are physically in another state.
7. The absence of agreed global cybersecurity frameworks hampers the development of a global privacy- and data protection framework.

8. The adoption of international trade agreements could also undermine the developing, global privacy- and data protection framework, unless it is made clear that restrictions on transborder data flows imposed to protect personal data shall not be regarded as “non-tariff barriers” to trade.

Recommendations

1. Where Telecommunication Regulators are involved in the enforcement of data protection laws (or elements of data protection laws), they should be independent and endowed with adequate powers, on the lines indicated in the “Model Laws”.

2. National policy makers should strive to revise and improve mutual legal assistance systems in relation to the obtaining of communications data from other countries for law enforcement purposes. The revised systems should fully respect privacy and data protection and include appropriate judicial safeguards.

3. Where cybersecurity laws or measures cover or touch on data protection (e.g., in relation to encryption or law enforcement of interference with communications or communication devices), they should respect the global data protection requirements.

Implementation of these recommendations will help to bring about the trust and security that consumers need, and that is the necessary foundation for the development of a global digital society.

Part 1: The broad context: Data, trust and security in the digital world

1.1 Introduction

Compared to a few decades ago, the overall environment within which governments, businesses and individuals operate and interact has changed fundamentally in technical terms. Computer processing power has continued to follow Moore's Law, with transistor density doubling every 18-24 months – around one thousand-fold in the last two decades. Computer storage capacity and communications bandwidth have both been increasing even more quickly, doubling every 12 months and hence a thousand-fold each decade.

These exponential increases have radically increased the ability of organisations to collect, store and process personal data. It is no surprise, therefore, that our world is increasingly saturated with sensors such as CCTV cameras and mobile phones, with biometric and electronic identifiers used to link data to individuals. In the digital world almost every communication, online activities such as payment, search and Web page access leaves behind detailed footprints.¹

Companies have long used data mining and -analysis to improve their products and services – and their margins. In a world of "Big Data" and the massive generation of both non-personal statistical- and personally identifiable data in the "Internet of Things" (IoT)² enables evermore detailed (and evermore intrusive) mining and "profiling". Governments are increasingly adopting similar technologies, in analysing and exchanging information on individuals in response to fears over terrorist attacks – or even over obesity in children.

The activities of both companies and governments in these respects has also become increasingly transnational: the digital environment by its very nature is global; and the economic opportunities and societal risks both also increasingly require transnational cooperation – between companies (the new environment is built on increasingly complex chains of actors); between governments; and between companies and governments. These developments pose serious challenges in terms of consumer protection³ and, indeed, to the maintaining of the Rule of Law in this environment generally.⁴

A 2016 ITU Report already noted the major monetary and economic impacts of the IoT, running to trillions of dollars annually within a decade; the societal impacts in particular in terms of "smart cities" with "smartly" controlled infrastructure, transport and buildings using "smart" meters, etc.; the impacts on individuals in terms of health- and care management (through IoT-enabled health devices). But it also stressed the major challenges in terms of costs and reliability, connectivity, user interfaces and addressing, and the regulatory implications of licensing and spectrum management, standards (including on interoperability), competition and customer lock-in, security and privacy.⁵

The paper seeks to provide a basis for discussion on how to maintain trust in a connected digital society. It does not seek to provide answers to the numerous questions and challenges relating to the global smart society, but it will explore major areas that deserve attention, with some very tentative suggestions about how progress could be achieved at the global regulatory level.

More in particular, the paper will discuss the special rules that apply to the processing of the personal data which lies at the core of the digital connected society. It looks at privacy and data protection rules (and at the differences between these concepts); at three core areas affecting trust and security in the digital environment: national security, public security and

cybersecurity, and international trade agreements in globalized seamless world; and at the roles and responsibilities of regulators in all these fields, and the relationships between them.

These are extremely complex issues, which the paper does not seek to resolve but rather to stimulate the discussion in an informed manner.

1.2 Consumer trust and technical security

The challenges posed by the new global digital environment will not be met, and the promised benefits of the IoT will not be reaped, unless two fundamental and related conditions will be fulfilled, globally: trust and security.

Consumer trust – or the lack of it – in the new digital environment has been identified in Europe as one of the main obstacles to the development of the Single Digital Market in the European Union⁶ – and the same is undoubtedly true in relation to the even wider global digital commercial environment. However, a 2014 survey conducted by Accenture found that globally, only 45 percent of consumers have confidence in the security of their personal data and that there are variations in the level of trust with developed markets expressing less digital trust overall. Consumers in emerging markets, in particular in Latin America and Asia, are more trusting, with 50 percent having confidence in the security of personal data compared to 41 percent of consumers in developed markets⁷.

These statistics are worrying as they suggest that as consumers are more exposed to the digital environment, their trust actually decreases.

Until consumers and citizens feel that they can trust the technologies of the new digital environment – that they are technically protected against online “identity theft”, financial fraud, data breaches, privacy violations and other misuses and abuses of their personal data⁸ – the administrative and economic benefits of the IoT and the wider digital environment will not fully materialise.

Trust thus, to a large extent, relies on security: security against technical failures and against deliberate attacks on the IT/IoT infrastructure – but also against undue interference with that infrastructure by official entities. If the technologies are unreliable – e.g., if “things” that are supposed to be interoperable in practice cannot “talk” to each other; or if systems go down and cannot be relied on – officials, businesses and citizens/consumers will rightly refuse to adopt them. If systems can be broken into by criminals and those criminals can help themselves to our money or our sensitive data, then we will not use those systems.

And if governments themselves undermine the security of the digital environment – e.g., by the installation of unsupervised “back doors” systems that could be subverted, or by breaking encryption codes or demanding the handing over of decryption keys in secret – then even upright citizens will shy away from the use of such systems unless they believe – trust – that such extraordinary powers are only used when manifestly justified, in a targeted rather than indiscriminate (“generalised”) manner,⁹ and with the strongest possible systems of authorisation and oversight. If the Rule of Law is either generally traduced in a country, or if (even in states that generally respect the Rule of Law) sections of the state – such as the security- and intelligence agencies – are felt to be above the Rule of Law and/or insufficiently open controlled, then again the citizen will not feel secure.¹⁰

1.3 Consumer trust and the regulatory framework

Consumer trust requires technical security and reliability. But it also requires a sound regulatory framework: sound regulations; good rules (including appropriately limited exceptions); and full and honest application and enforcement of those rules and regulations (and exceptions). However, Members of Consumers International, a global federation of consumer groups, have expressed serious concerns in this regard, with 80% feeling legislation and regulation relating to redress are ineffective at keeping pace with the digital economy, and 76% doubting the efficacy of enforcement.¹¹ In the remainder of this paper, we will look at some of the core issues relating to these concerns.

In the next part, Part 2, we will discuss the special rules and regulations that apply to the processing of the personal data which lies at the core of the digital connected society, i.e., at privacy and data protection rules (and at the differences between these concepts). In Part 3, we will look at a number of other core areas affecting trust and security in the digital environment: national security, public security and cybersecurity. And in Part 4, we will examine the roles and responsibilities of regulators in all these fields, and the relationships between them.

Part 2: Privacy, data protection, universality and free data flows

2.1 Global challenges; different concepts and approaches

The provision of digital services, Big Data and the IoT all centre on data, and increasingly on the linking of those data to the activities of individuals – be those consumers, employees or citizens (e.g., in self-quantification or staff- or consumption monitoring) or (possible) suspects (as in data mining and profiling by law enforcement- and national security agencies). The digital connected society runs on personally identifiable information (PII) or, as it is called in Europe, personal data. This often – and again increasingly – includes sensitive data, either directly, as in IoT-connected medical devices, or less obviously, e.g., through traffic- or location data that can reveal whether a specific person was at a specific place or meeting at a specific time, and with whom she interacted; or through Passenger Name Records (PNR) that can provide surprisingly revealing details of a person's health, religion or race (amongst other information).

In these regards, it should be noted that more and more data that might seem to be “non-personal” or that are said to have been “anonymised” can increasingly easily be (re-)linked to specific individuals. “Smart” electricity meters not only record statistics on usage over time – when analysed, the data can be surprisingly revealing about the occupiers of the house in question.¹² Data in supposedly “anonymous” “Big Data” datasets are unexpectedly, and worryingly, re-identifiable. Furthermore, if even truly non-personal datasets are used to create “profiles” (be that of typical consumers of a particular product, or typical patients, or typical criminals or terrorists), and those profiles are then applied to datasets to single out individuals that meet the profile – then that processing too can very seriously affect those individuals, who may be denied insurance, or a job, or access to a flight or even a country (or worse) on the basis of effectively unchallengeable algorithms.¹³

This raises fundamental questions about the rights of the individuals concerned. However, there are challenges even with the very phrasing of the issues, and of the rights concerned.

Specifically, as explained at 2.2., below, although they are closely related, there are conceptual differences between privacy and data protection that, in the global digital environment, cause tensions between states and hamper transnational regulation and enforcement and cross-border trade. These tensions and problems are further aggravated by historical differences in the protection of individual rights, in particular in relation to non-citizens and in the importance attached to the protection of personal data in different countries and regions (as discussed in section 2.3). In section 2.4, we will examine the extent to which the data protection instruments themselves offer possible solutions to these problems.

Two further complicating factors – different views on the depth of interference with privacy that can or should be permitted in the name of national security, public security and cybersecurity; and the possibility of international trade agreements overriding data protection – are discussed in Part 3.

2.2 Privacy and data protection

Historically, privacy was mainly concerned with the right of individuals “to be left alone” by other individuals or private entities such as newspapers.¹⁴ This was also generally the way the right to privacy and the “right to respect for private ... life” that are enshrined in the post-World War II UN International Covenant on Civil and Political Rights (1966) and other international human rights treaties were originally seen: as a limited, essentially “negative” right, imposing on the state (and to some extent, indirectly, on private entities) little more than a duty to refrain from interfering with the private sphere of individuals.¹⁵

From the 1970s, in the light of perceived threats of large-scale computerised (mainframe) databases, mainly in the hands of governments, some states began to develop wider concepts, aimed at countering this new threat – but less so on the basis of a perceived threat to privacy in the old sense (freedom from intrusion) than on the basis of a new view that it was wrong for individuals to be controlled by these new technologies. If privacy was about a right to be “left alone”, the new right, data protection, was about power. It sought, and seeks, to protect individuals from those who hold information on them using that information to manipulate and control them. The fear was that the computer could be used to undermine human autonomy and personal freedom in broad senses and, if done on a wider scale, could undermine democracy and freedom itself. As it is put succinctly in one of the earliest (1978) national data protection laws in the world, France’s *Law on Informatics, Files and Freedoms*:¹⁶

Computer technology ... may neither infringe human identity nor the rights of man, nor private life, nor private or public liberties.

Data protection in this wider sense – of a *sui generis* right to protection of “data subjects” against improper uses of their data by those owning those data (“data controllers”) – is particularly strongly embedded in European law including the European Convention on Human Rights and the European Union’s Charter of Fundamental Rights, as interpreted and applied by the European Courts (the European Court of Human Rights and the Court of Justice of the EU). However, as noted in the next section, it is increasingly adopted worldwide and reflected in many guidelines and model laws being discussed globally, and can therefore serve as a reference to develop a regulatory framework for the global digital connected society.

However, before discussing the global data protection instruments as such, it is important to note another major factor that impacts on the application and enforcement of privacy/data protection law in the global digital environment: the general historical move from citizens’ rights to universal human rights.

2.3 Universality of human rights

It is one of the hallmarks of international human rights law since 1945, and one of its greatest achievements, that under modern human rights treaties and constitutions such rights must be accorded by states to “everyone”, to all human beings within the “jurisdiction” of that state, “without distinction [or discrimination] of any kind”,¹⁷ including nationality or legal residence status – rather than just to citizens of a state, as often used to be the case, in particular under constitutions adopted in earlier centuries.¹⁸

Moreover, the concept of “jurisdiction” as used in the modern human rights treaties has been developed from a purely territorial one – under which the rights in question must be accorded to everyone on the territory of the state concerned (only) – to one that relates to the exercise of power. According to the modern view of human rights, as pronounced by the International

Court of Justice as well as by global and regional human rights courts and -fora, states must accord (almost) all the rights contained in the human rights treaties to which they are a party, to everyone over whom they in some way hold power, i.e., in respect of whom they *exercise* jurisdiction (including prescriptive and enforcement jurisdiction).¹⁹

More specifically, this means that when states or state agencies or -agents are active in the (by its nature transnational) digital environment, they are bound under international human rights law to respect those rights, also in relation to any effect their actions may have on people who are physically outside of the territory of the state concerned.²⁰ Indeed, under the doctrine of “horizontal effect” of human rights,²¹ they are also required to ensure that private entities such as companies that are subject to their laws are also prevented from actions that would unduly interfere with the protected rights of the persons concerned – including foreigners physically outside the country in question.

Some states have not yet adopted this “universal” view of human rights in their domestic law – which is challenging in the digital environment, especially if such states take actions in the global digital environment (e.g., “tapping” into the global submarine cable communications network) that clearly affect the rights and interests of consumers and citizens elsewhere in the world.²² As illustrated by the Snowden case, this has serious negative effects on the global regulatory system, as discussed in Part 4.

2.4 The regulation of global personal data flows in the main international data protection instruments and model laws

2.4.1 *The dilemma*

When (initially only European) countries began to adopt data protection laws in the late-1970s and -80s, these naturally imposed restrictions on the free flow of personal data to other countries, so as to avoid evasion of the rules. This posed a dilemma that persists to this day.

On the one hand, the free flow of data, including personal data, “contribute[s] to economic and social progress [and] trade expansion” and facilitates cooperation between public authorities in different countries as well as scientific and technical cooperation and improved telecommunication, which is all of benefit to both companies and individuals. On the other hand, for countries and regional bodies that accept that data protection is a fundamental right, the processing of personal data involved in this must respect that right “whatever the nationality or residence of [the persons concerned].”²³

If there are “a wide variety of national laws, regulations and administrative provisions” on the processing of personal data, establishing different levels of protection for such data (or if there are countries without any relevant law, providing no protection at all), this “may prevent the transmission of such data from the territory of one [country] to that of another [country]”, and this difference can “constitute an obstacle to the pursuit of a number of economic activities” at the trans- and international level, “distort competition” and “impede authorities in the discharge of their responsibilities”.²⁴

A range of attempts have been made to resolve this dilemma. In the 1980s, first the OECD and then the UN adopted non-binding guidelines, with the recommendation that as long as countries “substantially” or “broadly” followed these guidelines in their laws or regulations (or even through self-regulation), other countries should not impede personal data flowing

to them. More recently, APEC has adopted a Privacy Framework that is also non-binding and relatively flexible in respect of transborder data flows.

The Council of Europe went further and already in 1981 adopted and opened up for signature a binding international convention on data protection, which is expressly open to non-Council of Europe states. This contains stricter, binding rules than the above-mentioned guidelines, also in respect of transborder data flows. It has been supplemented by an additional protocol and is also more generally being “modernised”.

The most detailed and strictest rules were adopted by the European Union, in a range of data protection instruments that are now firmly linked to the right to data protection as enshrined in the EU Charter of Fundamental Rights, which (since the coming into force of the Lisbon Treaty) has binding – and indeed constitutional – status within the EU legal order. These instruments also impose strict rules on transfers of personal data to non-EU (and non-EEA) countries, if those countries do not offer “adequate” protection to the data. The Court of Justice of the EU has recently ruled that, because of the high status of data protection in the EU legal order, this “adequacy” requirement should be read as demanding that the other country in fact offers “essentially equivalent” protection to that required under the Charter. In addition, the EU rules contain important provisions extending the application of those rules to non-EU/EEA companies that offer goods or services to EU persons, or that “monitor the behaviour” of such persons, in particular online.

The European rules have been hugely influential globally. More than 100 countries have adopted data protection laws, many specifically drafted on the lines of the EU rules. This latter development has been facilitated in particular by the promotion by a number of regional organisations of “model laws” based on the EU rules and drafted with the assistance of the EU.

In this section, we will first, in the next sub-section, 2.4.2, describe the non-binding UN-, OECD- and APEC guidelines. In sub-section 2.4.3, we will look at the binding Council of Europe and EU instruments; and in sub-section 2.4.4, at the model laws. In sub-section 2.4.5, we will discuss the special problem of jurisdiction in the digital environment, as concerns data protection. In the final sub-section, 2.4.6, we will examine the prospects for a global framework.

We will focus on the rules on transborder data flows, while noting in more general terms the different levels of detail and strictness in the different rules (in particular, in the binding instruments compared to the non-binding recommendations), since these impact on the transborder data flows.

2.4.2 Non-binding guidelines

Non-binding guidelines have been adopted by the United Nations, the OECD and the Asia-Pacific Economic Community (APEC).

The first of these was the 1980 OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data.²⁵ These were revised in 2013 in the context of the creation of a wider OECD Privacy Framework that also includes new rules on privacy enforcement cooperation (that built on a 2007 recommendation on the issue).²⁶

Some years later, in 1989, the UN adopted its own Guidelines for the Regulation of Computerized Personal Data Files.²⁷

Most recently, in 2004, the Asia-Pacific Economic Community (APEC) published its Privacy Framework,²⁸ strengthened in 2007 by an APEC Cross-border Privacy Enforcement Arrangement (CPEA), further discussed in Part 4.²⁹

With some variations, all of these share a set of common principles, which also lie at the basis of the binding instruments discussed at 2.1.2, below, as illustrated below:³⁰



Source: UNCTAD /data protection regulations and international data flow: implications for trade and development http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

All three instruments seek to facilitate free data flows between states that have signed up to the relevant principles, as long as they broadly follow these – themselves already quite broadly-phrased – principles. As stated in the OECD Guidelines, “A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country **substantially observes** these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines (Para. 17, emphasis added)”.

The UN and APEC guidelines follow similarly flexible broad principles: they all allow for quite different privacy and data protection systems – yet are aimed at mutual recognition of the adequacy of those different systems, as long they broadly meet the broad principles. Provided they follow these guidelines, the Member States of these organisations are encouraged to allow free data flows between them.

2.4.3 Binding regional data protection instruments with international reach

The first binding international instrument in the field of data protection was the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, better known as the Data Protection Convention (DPC) or “Convention No. 108” after its number in the European Treaties Series,³¹ which in 2001 was augmented by an Additional Protocol regarding supervisory authorities and transborder data flows.³²³³ As already mentioned, the Convention is in the process of being “modernised”. The “Ad hoc Committee on Data Protection” (CAHDATA) appointed to this end has produced a Working Document with a Draft Protocol on the proposed amendments, which will to a large extent bring the Convention into line with the EU rules, noted next.³⁴

In between the adoption of the Council of Europe Data Protection Convention in 1981 and the adoption of the Additional Protocol to that Convention in 2001, the European Union adopted, in 1995, the Data Protection Directive (or DPD for short).³⁵ A subsidiary directive on data protection in the field of electronic communications, known as the e-Privacy Directive, was further adopted in 2002.³⁶

On 14 April 2016, the European Parliament approved, after a long legislative history, a new EU General Data Protection Regulation to replace the 1995 Data Protection Directive.³⁷ The new regulation is more detailed and strict than the 1995 directive and will be more uniformly interpreted and applied, through a number of new processes called the “cooperation-”, “mutual assistance-” and “consistency mechanisms”. It contains important provisions that are stricter in terms of extraterritorial effect and transfers of data to non-EU (and non-EEA) countries. Although the new regulation will not come into full effect until May 2018, it is already casting its shadow forward.

At almost the same time, on 11 April 2016, the Commission launched a consultation on its revision of the e-Privacy Directive, in which it will look at “possible changes to the existing legal framework to make sure it is up to date with the new challenges of the digital area.”³⁸

The EU has also adopted, or is in the process of adopting, a range of instruments on the processing of personal data by law enforcement agencies in the EU, and on the transfer and sharing of data for law enforcement purposes that have proved to be highly contentious, in particular in the light of a number of important judgments from the European Courts.

The requirements of the European instruments cannot be discussed here in detail. However, three aspects of direct relevance to the global digital connected world are described below.³⁹

First, as noted at 2.2, above, data protection in a broad sense is regarded throughout Europe as a fundamental, universal human right.⁴⁰ In terms of EU law, it follows that personal data may only be transferred to another country if that other country provides protection that is “essentially equivalent” to the European standards, both in terms of substance and in terms of the availability of real and effective remedies.⁴¹ Moreover, this protection must be provided by “the legal order” of the country in question;⁴² and it must provide for effective remedies for “everyone” (i.e., not just for some categories of individuals, like nationals of specified countries).⁴³ The legal order of the other country must also protect against undue collection of data in bulk – and may in any case not provide for “generalised” – i.e., indiscriminate – access by the country’s authorities to the content of communications.⁴⁴ These restrictive transfer requirements of EU data protection law are expressly allowed under the proposed revised text of the Council of Europe Data Protection Convention.⁴⁵

However, the Regulation also envisages the provision of “suitable safeguards” by companies or groups of companies or sectoral bodies, in the form of data transfer contracts, Binding Corporate Rules or (typically sectoral) Codes of Conduct, subject to approval of such instruments by the data protection authorities (or at the European level, by the newly-established European Data Protection Board).⁴⁶ The EU Commission and (subject to EU-level approval) the national authorities can also issue “standard transfer contracts” (and have already done so under the 1995 Directive); and suitable safeguards for transfers can also be provided through privacy seals, through newly-regulated certification mechanisms. While there are still many questions about the operation of these mechanisms, they might provide the means to link the new European rules to the wider, global data protection regime (as noted in the next sub-section). The proposed revised text of the Council of Europe Data Protection Convention again expressly (albeit in broader terms) confirms this approach.⁴⁷

Second, although they are built on the same “core principles” as the non-binding UN-, OECD and APEC guidelines, the European instruments are much more detailed and strict – the new EU General Data Protection Regulation alone runs to 149 pages of small print, with 99 long articles with numerous sub-clauses. They are, moreover, supplemented by very extensive, even more detailed recommendations and guidance from specialised bodies that generally further interpret the rules strictly.⁴⁸

Third, it is an EU Charter requirement that the implementation of data protection law in the EU Member States be supervised by an independent authority. In several cases, the EU Court of Justice has underlined that data protection supervisory authorities have to remain free from any external influence, including the direct or indirect influence of the state; and indeed that the mere risk of political influence through state scrutiny is sufficient to hinder the independent performance of the supervisory authority's tasks.⁴⁹ The GDPR sets high standards for the relevant regulators in this regard;⁵⁰ specifies the tasks they must be authorised to perform, including handling complaints and carrying out investigations of their own motion;⁵¹ and also requires that they be vested with very extensive powers of enforcement, including:⁵²

- carrying out investigations and data protection audits;
- demanding access to premises and equipment used in processing;
- issuing warnings, reprimands and if needs be orders to data controllers;
- imposing “a temporary or definitive limitation including a ban on processing”;
- ordering the suspension of data flows to recipient in non-EU countries; and
- imposing “administrative fines” for non-compliance with the Regulation or such orders, of up to 4% of annual turnover of the controller.

The Additional Protocol to the Council of Europe Data Protection Convention also requires the establishment of an independent data protection authority with broad powers and the proposed revised text of the Convention (if adopted as drafted) will bring this requirement into the main Convention framework.⁵³ As noted in sub-section 2.4.6, below, and in Part 4, this has implications for the nascent global data protection regime.

2.4.4 Model laws

Both the Council of Europe and the European Union have given extensive assistance to many non-European countries in the drafting of privacy- and data protection laws, drawing on the European instruments (the Council of Europe Data Protection Convention and the EU Data Protection Directive) discussed above.

Moreover, within a global ITU-EU-ACP project, the ITU and the EU (and others) have undertaken extensive work towards the establishment of harmonised policies for the ICT market in the African, Caribbean and Pacific (ACP) countries. This has resulted in the writing of a number of “Model Laws” and guides governing data protection (and others covering cybercrime and other matters). These include, specifically:

- HIPCAR: Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean:⁵⁴
Privacy and Data Protection: Model Policy Guidelines & Model Legislative Texts (2012)
- HIPSSA: Harmonization of ICT Policies in Sub-Saharan Africa:
Southern African Development Community (SADC):⁵⁵
SADC Data Protection Model Law (2013)
- Model Laws Project of the Economic Community of Central African States (ECCAS) & Directive Project of the Economic and Monetary Union of Central Africa (CEMAC):⁵⁶
Model Law/Directive Relating to the Protection of Personal Data (2013)
(contained within a broader publication on Cybersecurity Regulation)

All the above “model” instruments are clearly inspired, in terms of definitions, core principles, even structure and specific issues addressed, by the European data protection rules, in particular the 1995 EU Data Protection Directive.

Notably, they all also adopt the basic approach of the EU data protection instruments in relation to transfers of personal data to other countries: they stipulate that such transfers should in principle be prohibited unless the other country in question has adopted a law on the basis of the relevant Model Law, or otherwise ensures “comparable levels” of protection/an “adequate level” of protection, while also allowing for alternative means of providing safeguards, in particular through contract clauses.⁵⁷

2.4.5 Jurisdiction

The question of jurisdiction is a major general problem in the inherently frontierless digital environment.⁵⁸ As the renowned Professor of Law Teresa Scassa and Robert J. Currie put it: “because the Internet is borderless, states are faced with the need to regulate conduct or subject matter in contexts where the territorial nexus is only partial and in some cases uncertain. This immediately represents a challenge to the Westphalian model of exclusive territorial state sovereignty under international law.”⁵⁹

In relation to data protection, the three main (linked) issues are:

- i. The duty of states to ensure data protection to anyone “within their jurisdiction”;
- ii. The application of national data protection laws extraterritorially to activities by people or companies – or even public bodies – in other states; and
- iii. The increasingly common cross-border “pulling” of personal data by one state’s agencies from servers or devices that are physically in another state.

Briefly, the following may be noted in respect of these three issues:

Re i.: In sub-section 4.2.3, above, we have already shown that under modern human rights law, states have a duty to apply privacy- and data protection safeguards to “everyone within their jurisdiction”, and that the latter term is now given a functional rather than a territorial meaning (even if some states do not apply it).

This widely-interpreted “jurisdictional” duty is clearly expressed in EU law (both in the Charter of Fundamental Rights and in the data protection rules). The EU guarantees data protection to “**everyone**” affected by any processing of their personal data by EU-based controllers, irrespective of where the affected persons (data subjects) are.

The Council of Europe Convention, in its original (still current) 1981 version is still restrictive in this regard; it stipulates that its purpose is to secure data protection rights for every individual “**in the territory of each Party**” (Article 1). These words have however been deliberately deleted from the proposed new “modernised” text of the same article. This must now be read together with the proposed new Article 3(1), which stipulates that:

Each Party undertakes to apply this Convention to data processing **subject to its jurisdiction** in the public and private sectors, thereby securing every individual’s right to protection of his or her personal data.

Specifically, in the wider Council of Europe area, too, the term “jurisdiction” must be read in functional rather than geographical terms, if only because the European Court of Human Rights has given the term such a wider application (see again sub-section 4.2.3, above).

The non-binding guidelines are by their nature less clear on this issue – but the OECD Guidelines reflect some of the same thinking where they stipulate that a data controller remains accountable for personal data under its control without regard to the location of the data (paragraph 16).

The Model Laws all also basically reflect the modern, broad view of the need to extend data protection to everyone affected by a state’s action.

Re ii.: The non-binding UN-, OECD- and APEC guidelines are essentially silent on the question of whether, and if so when, states can extend the application of any laws adopted on their bases to actions by people, companies or public bodies in other states.

By contrast, the 1995 EU Data Protection Directive requires all EU Member States to apply their data protection laws to any company headquartered outside the EU if it sets up an establishment in an EU Member State, when this local establishment “orientates its activity towards the inhabitants of that Member State” (Article 4(1)(a) as interpreted in the *Google Spain* judgment of the CJEU, the so-called “Right To Be Forgotten” case).⁶⁰ The Directive also requires Member States to apply their law to any non-EU company (even without an establishment in their territory) which uses “equipment” or “means” in their territory to

process (e.g., collect) personal data on individuals in the EU (Article 4(1)(c)).⁶¹ It is not entirely clear when this can be said to be the case, but the Article 29 Working Party has held that this can include the use of agents (physical or legal persons) as well as the use of cookies or Javascript banners (as long as this is not applied in cases with only tenuous links to the EU).⁶²

The just-adopted General Data Protection Regulation clarifies and extends this further: Article 3(2) stipulates the following:

This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

- (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
- (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

In relation to the Internet, “monitoring of the behaviour” of consumers in the EU can be said to take place in particular if the company uses “tracker cookies” or other online tracking tools.

The Model Laws, being generally inspired by the 1995 EC Data Protection Directive, tend to follow the approach of that directive. Thus, the HIPCAR Model Legislative Text on Privacy and Data Protection stipulates in Article 5 that:

This Act applies to a the [sic] Data Controller in respect of any data if –

- a. the Data Controller is established (ordinarily resident, incorporated or branch office) in [Name of Member State] and the data is processed in the context of the business of that establishment; or
- b. the Data Controller is not established in [Name of Member State] but uses equipment in [Name of Member State] for processing data otherwise than for the purpose of transit through [Name of Member State].

This follows Article 4 of the Directive almost *verbatim*. Note in particular the reference in Article 5(a) to “branch office”, which echoes the CJEU *Google Spain* approach. The reference to “equipment in Article 5(b) appears to be the result of the Model Legislative Text being based on the English language version of the EC Directive.

Re iii.: It is becoming increasingly common for state agencies – in particular law enforcement and national security agencies – to use the global digital infrastructure to “pull” data directly from servers or devices in other countries, without using the traditional processes under Mutual Legal Assistance Treaties (MLATs), or indeed without in any other way having obtained the consent of the targeted state. This is highly dubious in terms of general public international law, in that (outside times of war) such actions constitute the exercise of “enforcement jurisdiction” in another country, which violates the sovereignty of the other country.⁶³ Indeed, in cybercrime law, such unauthorised “equipment- or device interference” is now almost universally regarded as a criminal offence. Agents of the state making it a criminal offence may be granted special exemptions (e.g., in rules allowing law enforcement bodies to intercept communications subject to certain substantive and procedural requirements), but those do not normally extend to actions by foreign agencies. As explained elsewhere, Article 32 of the Council of Europe Cybercrime Convention (also known as the

Budapest Convention), which seems to permit such cross-border “pulling” of data, was never intended to be routinely used for such purposes.⁶⁴

In this regard, there is something of a conflict between law and practice. On the one hand, as just noted, it would appear that such practices are contrary to international law. On the other hand, if anything those practices are spreading (or at least are becoming increasingly exposed in the wake of the Snowden revelations). Yet it cannot be argued that this widespread practice constitutes (the beginning of) new customary law, because there is no *opinion iuris*: although many states engage in the practices, there are few clear statements to the effect that they are accepted as lawful. On the contrary: most states at the receiving end of such practices protest strongly when such activities of foreign agencies are exposed. That is the opposite of accepting the practice as lawful.

In sum:

- i. States are increasingly adopting national or regional data protection laws that extend data protection to everyone affected by a state’s action, even if the affected persons are outside the physical territory of the state in question;
- ii. States are increasingly adopting national or regional data protection laws that extend their application also to activities of foreign companies if those foreign companies either have an establishment in the country concerned or use “equipment” in the country in question to process (and in particular to collect) personal data on people in that country;
yet:
- iii. States are also still allowing or at least condoning cross-border data-“pulling” activities by their law enforcement and national security agencies that appear to be *prima facie* in breach of public international law and that also unlawfully interfere with the privacy- and data protection laws and rights of the foreigners affected.

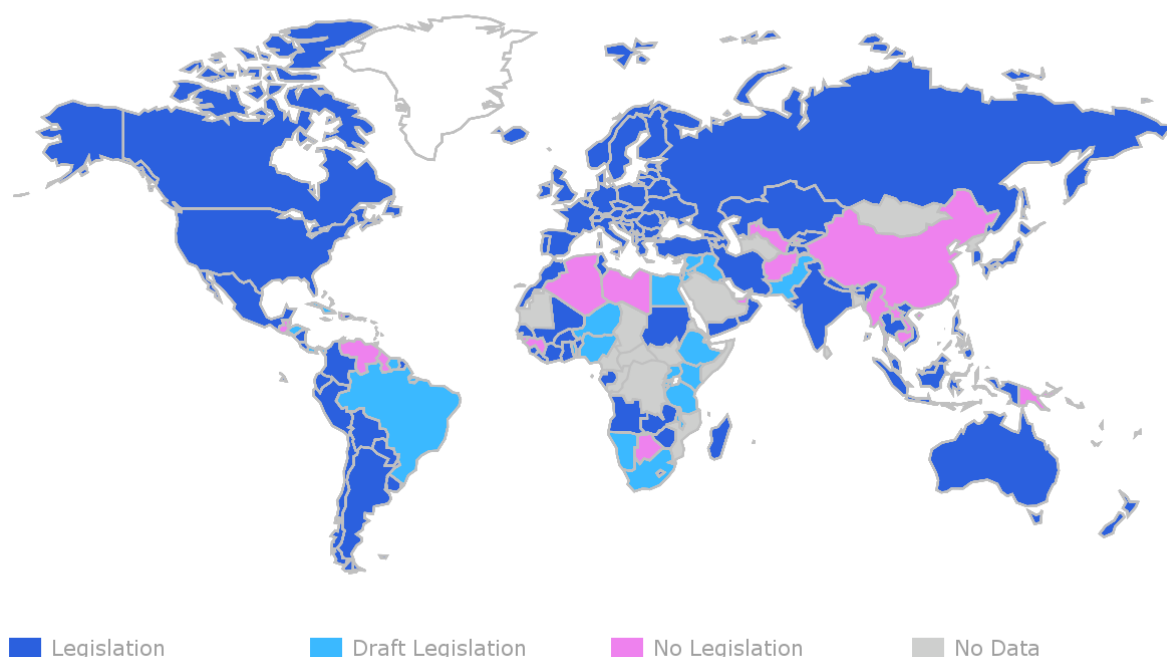
We will return to the latter issue in Part 4.

2.4.6 Data protection: global convergence and cooperation

The laws in many countries are clearly inspired by, and often closely modelled on, the European instruments, the 1995 EU Data Protection Directive in particular. Overall, more than 100 countries have adopted privacy- or data protection laws, as shown overleaf,⁶⁵ and it would appear that over time these are being strengthened in the direction of the “European” standards. A recent UNCTAD report⁶⁶ noted that governments “specifically in those developing countries attempting to adopt data protection legislation – are having problems modelling their data protection regimes, though most opt for an approach consistent with the EU Directive”.

The Council of Europe Data Protection Convention – which has in any case been ratified by all the organisation’s 47 Member States⁶⁷ – is open to all countries in the world and has in fact been acceded to by Uruguay; four African states are due to also become full parties to it: Mauritius, Morocco, Senegal and Tunisia. More are expected to join in the coming few years, in particular once its “modernisation” is concluded. Six non-EU states (Andorra, Argentina, Australia, Canada, Switzerland and Israel) have been formally declared to provide privacy rules that are “adequate” in terms of the EU rules.

Data Protection and Privacy Legislation Worldwide



Source: UNCTAD, 14/04/2016

This trend is reinforced by increasing support for stronger global privacy- and data protection laws given by the global intergovernmental- and human rights bodies. In the wake of the Snowden revelations, the UN General Assembly adopted a resolution on the issue in 2013,⁶⁸ which led to a report by the High Commissioner for Human Rights on the promotion and protection of the right to privacy in the digital age⁶⁹ and the appointment of the new UN Special Rapporteur on Privacy, Joseph Cannataci.⁷⁰

The Revised OECD Privacy Framework and its guidelines have, over the years, been implemented increasingly strictly and in more detail. While the Revised OECD Privacy Guidelines still stipulate that Member countries should refrain from restricting transborder data flows to other countries that “substantially observe” the Guidelines, they also strongly encourage the adoption of appropriate safeguards. As the Supplementary Explanatory Memorandum to the 2013 Revised Guidelines put it, with reference to Article 17(b):⁷¹

[This paragraph] gives recognition to the measures which a data controller can put in place to ensure a continuing level of protection, which may result from a combination of measures, such as technical and organisational security safeguards, contracts, complaint handling processes, audits, etc.

However, the measures provided by the data controller need to be sufficient and supplemented by mechanisms that can ensure effective enforcement in the event these measures prove ineffective.

Paragraph 17(b) therefore includes as a consideration the availability of effective enforcement mechanisms which support measures adopted by the data controller. Such enforcement mechanisms may take a variety of forms, including for example, administrative and judicial oversight, as well as crossborder co-operation among privacy enforcement authorities.

The reference to the need for “effective enforcement mechanisms” clearly relates to the fact that the existence of such mechanisms is seen as crucial in the EU rules and the Additional Protocol to the Council of Europe Convention (which will be brought within the main text of the Convention in the “modernisation” process).

From the EU’s side, Article 50 GDPR expressly requires the EU Commission and the data protection authorities of the EU Member States to be active in this regard:

EU Data Protection Authorities must:

- develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;
- provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
- engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data; and
- promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

There is therefore clearly at least the beginning of some convergence in terms of the contents of and approaches in data protection laws, with a trend towards adoption of laws on the “European” lines (cf. also the first two points in the summary at the end of the previous subsection). And there is strong global support for closer and more effective cross-border cooperation. It may be hoped that once it is revised and “modernised”, the Council of Europe Data Protection Convention, which as mentioned is open to all states (not just to European ones) can become a global reference for data protection on which mutual assistance and mutual recognitions can be built. In other words, a tentative global framework is slowly emerging. This will be further discussed in Part 4.

The next section, part 3, will examine the scope and range and cross-border application of special rules relating to national security, public security and cybersecurity (and indeed the lack of clarity with regards to these very concepts); and trade agreements, that all impact on privacy and data protection globally.

Part 3: National security, public security and cybersecurity, and trade agreements

There are two broad threats to the development of the global framework noted in Part 2:

- laws and measures in many countries that are aimed at the protection of national security, public security and cybersecurity often allow for very broad interferences with privacy and data protection, in widely varying ways and extents;
and
- a series of proposed trade agreements which, their opponents argue, allow data protection laws (and other laws with socially beneficial aims such as protection of health and the environment) to be set aside if they threaten profits.

The challenges should be noted before we discuss the future regulatory possibilities and difficulties.

Connectivity in a digital world also brings with it vulnerabilities at all levels and in all layers: in infrastructure and networks, transmission systems, hosting (clouds), apps and existing and innovative new systems and services (such as virtualisation and “softwarisation”) and devices. Governments, businesses and individuals all seek protection against breakdowns, cyberattacks, fraud, data misuse, etc. – and as already noted, will not trust the digital environment until such protections are in place.

Protection in the digital world comes broadly in two forms: technical protection, and legal protection. These interrelate in that the law can stipulate or encourage the adoption of technical measures, set technical standards, and establish regulatory systems and - authorities. But the law can also allow for interferences with technical protection measures if these are believed to protect the wrong people: criminals, terrorists – and other, even less-defined targets. And it can either protect, or fail to protect, against abuses of technical measures that can have undue effects on the rights of individuals.

This poses serious dilemmas at national and international level, which have not yet been resolved.

Thus, on the one hand, security (e.g., against online and offline bank card fraud, or the physical security of an airport) can be enhanced by secure identification and authentication – which increasingly involves the use of advanced biometrics. But there are inherent dangers in the use of biometrics – including the uncontrolled matching of data from different sources, the surreptitious monitoring of individuals, and possible discrimination.⁷²

There is also the question of whether individuals have a right to anonymity in the online environment. On the one hand, this allows people to access information on issues that may be contentious in their places of residence: e.g., political, religious, sexual or medical. Without protection of their identity, people in many countries would face serious consequences for even looking at such material. On the other hand, it allows “internet trolls” to post defamatory or threatening statements or material on the web, and religious and political extremists to disseminate hate speech and calls for violence, without risk of exposure for themselves.

Similarly, fully secure, unbreakable encryption allows citizens to feel confident in communicating and exchanging data and information with each other and supporting people and organisations worldwide; increases consumers’ willingness to conduct more online

activities such as making payments, exchanging health records with their doctors, etc.; and enables whistleblowers to expose serious wrongdoings. But it also allows terrorists to plan their attacks in secret; and paedophiles to exchange images of child sex abuse. Yet breaking security and encryption risks breaking the whole security of the global digital environment: a vulnerability once detected and exploited by one actor (even a “good” one) can and will sooner or later be used by another (“bad”) one.

All the international instruments discussed in Part 2 acknowledge the need for restrictions on the rights to privacy and data protection, where such restrictions are needed to protect general societal interests.⁷³ They also acknowledge that such restrictions should be based on law and be kept to the minimum necessary. However, the precise implications of these requirements are not at all clear – and the exceptions are clearly applied differently in different countries according to their regulatory regimes.

Furthermore, the very concepts – the aims for which restrictions may be imposed – are often not clearly defined, either in the privacy/data protection instruments, or indeed in national and international law generally.

Thus, in many countries the concept of “national security” includes the fight against organised crime and the protection of the economic interests of the state; is left deliberately undefined; at the discretion of the authorities; or can include the prevention of incitement to commit (apparently any) offences.⁷⁴ National security and “intelligence” agencies may be authorised to not just counter terrorism and other major threats such as organised crime, but also to gather information for political and economic purposes (even in the absence of any threat).⁷⁵

“Public security” can similarly cover anything from serious and imminent threats to vague, non-criminal concerns; and “cybersecurity” is variously defined, by different organisations, to cover such diverse matters as:⁷⁶

- purely technical security issues (protection against non-criminal threats to IT infrastructure);
- “cybercrime” (which itself covers very different things, from interception of communications and “hacking” to child pornography and hate speech);⁷⁷
- the activities of law enforcement-, military- and intelligence agencies in cyberspace;
- some even add civil law and –procedure relating to e-contracts etc. –

The various sources also include in the concept of “cybercrime” anything relating to the above:

- in substantive law, procedure, oversight and remedies, national institutions, international instruments, and intergovernmental arrangements and –institutions;
- at the national and international/transnational level;
- and in national and international policy-making in these regards.

These conceptual issues are problematic because if there is no common, agreed understanding of the very concepts of “national security”, “public security” and “cybersecurity”, it will be impossible to arrange for good international regulatory cooperation on the measures taken to protect them.

In broad terms, individual-, human- and consumer rights are mostly obviously affected by measures taken by state and private entities to counter threats to national-, public- or cybersecurity in two main ways:

- if such measures involve monitoring of the activities of individuals in the digital online environment, the pulling of data on individuals (or that may also relate to individuals) from “cyberspace”,⁷⁸ and/or the storing, sharing, analysing and further using of such data (e.g., for “profiling”); and
- if such measures are taken as part of criminal investigations (or may lead to such investigations).

These matters are complex enough in any single domestic context. However, the requirements become both more complex and more demanding if:

- the measures involve cooperation – and data exchanges – between state and private entities (companies, including in particular companies active in the digital environment, such as Internet Service Providers (ISPs), mobile network operators (MNOs) and social network service providers (SNSs);
- the measures involve cooperation – and data exchanges – between law enforcement agencies and national security agencies; and
- if there are transnational/international aspects to the measures, i.e., if they either involve actions of entities in one country that directly affect individuals (the data of individuals and the rights of individuals) in other countries (such as the pulling of data from a server in one country for analysis in another country), or if they involve cooperation between entities in different countries (which could be cooperation between private entities in different countries, or cooperation between public entities in different countries [such as international law enforcement- or national security cooperation], or cooperation between private entities in one country and public entities in another country).

It becomes increasingly challenging when these factors add up.

From the citizens’ and consumers’ perspective issues of serious concerns include:

- The indiscriminate “hoovering up” or otherwise accessing of massive sets of “bulk data” by intelligence agencies for use in data mining and profiling, in order to single out people who may possibly be involved in terrorism or other serious crime; and by companies to target prospective clients (or identify potentially bad customers). Decisions based on such data mining and profiling are subject to serious limitations and risks for consumers and citizens, including the risks of discrimination and high levels of “false positives” (because of the “base-rate fallacy”), but become effectively unchallengeable since they are based on increasingly complex, secret algorithms.⁷⁹
- The installation of “back doors” into the servers and systems of electronic communication providers and others, through which state agencies have effectively uncontrolled full access to the data held and processed in and through those systems (i.e., without there being “data hand-over arrangements” as used to be in place in older systems), with “gagging orders” preventing the companies concerned from disclosing the existence of those doors, with severe penalties for any disclosure. They

also create vulnerabilities that can be exploited and thereby the security and reliability of the entire networks.⁸⁰

- Demands for the weakening of encryption and/or the compulsorily making available of decryption keys by major Internet companies, including “cloud” providers, to allow “exceptional access” to data by state agencies. If the authorities that demand such weakening of encryption and handing over of keys are successful, this will undermine the security of the entire global Internet and electronic communications infrastructure, including the financial-, trading and even defence infrastructures: “encryption cannot be weakened ‘just a little’”.⁸¹
- The increasing trend of law enforcement and national security agencies “pulling” data directly from servers and devices in other countries in order to obtain evidence or intelligence – without using the traditional means for cross-border investigations, so-called Mutual Legal Assistance Treaties or MLATs.⁸² This threatens to undermine both the established systems for mutual law enforcement assistance (although these do need urgent reform) and the emerging system of global data protection, discussed in Part 2, above.

International law, including international human rights law, on all these issues is still underdeveloped, but some of the basic principles and tests are beginning to be clarified in regional and international courts and other fora.

At the broader policy level, a number of organisations, including intergovernmental organisations, international defence-, trade- and financial organisations, academic institutions and major corporations are involved in a range of initiatives. This includes the ITU, which, with others, is in the process of producing a Cybersecurity Strategy Reference Guide and has already produced a Cybersecurity Strategy Toolkit;⁸³ the Global Cybersecurity Capacity Centre (GCCC) of the Oxford Martin School of the University of Oxford, which is working on a “Cybersecurity Maturity Model” (and which is also involved in the drafting of the Reference Guide);⁸⁴ and the Global Forum on Cyber Expertise (which includes both the ITU and the GCCC).⁸⁵

However, this work is still very much in its infancy, with the focus for now being on the development of broad policies and strategies rather than on “details” such as how exactly the rules on national security, public security and cybersecurity should interrelate with the rules on privacy and data protection discussed in Part 2. In particular, apart from the, in this regard not yet very clear, limits imposed by human rights law, there are, at the moment, effectively no international frameworks regulating the work of intelligence services.⁸⁶

Finally, we should mention proposed international trade agreements are currently being negotiated and which could impact on data protection. These include the proposed EU-USA Transatlantic Trade and Investment Partnership (TTIP),⁸⁷ the proposed EU-Canada Comprehensive Economic and Trade Agreement (CETA)⁸⁸, and the proposed Trans-Pacific Partnership (TPP) between the USA, Canada, Australia, New Zealand, Japan, Brunei, Malaysia, Singapore, Vietnam, Mexico, Chile and Peru.⁸⁹

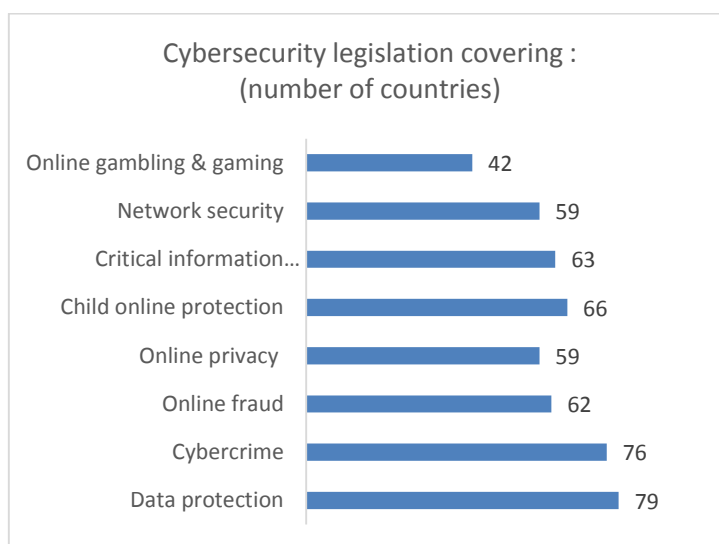
The debates generated by these proposed texts clearly highlight the importance citizens and consumers place in ensuring that these proposed trade agreements do not overrule data protection and privacy rights, in particular (but not only) in relation to transborder data flows and questions of jurisdiction.⁹⁰

In sum: The absence of agreed global cybersecurity- and intelligence frameworks hampers the development of a global privacy- and data protection framework; and the adoption of international trade agreements could also undermine the latter, developing, framework, unless it is made clear that restrictions on transborder data flows imposed to protect personal data shall not be regarded as “non-tariff barriers” to trade.

Part 4: Roles and responsibilities of regulators

4.1 Different and overlapping frameworks

Today, different regulatory instruments and frameworks are regulating the digital ecosystem. Various entities may be in charge of overseeing data protection, privacy and security.



Source: ITU ICT Eye

According to ITU data, 73% of countries worldwide have adopted cybersecurity legislation (i.e., legislation covering all or most of the above kinds of broad issues). As the above chart shows, in 79 countries, data protection measures are included in such wider laws, while 59 countries have laws specifically dealing with online privacy. Cybersecurity (in this broad sense) falls within the mandate of the telecom/ICT regulator in more than 55% of the countries worldwide. This is the case of nearly 80% of the countries in Africa, 64% of the countries in Asia-Pacific and 61% in the Arab States.⁹¹

In many other countries both the regulatory frameworks and the regulators may be more dispersed. In Europe, as noted in Part 2, above, and further discussed below, at 4.1.2, special data protection laws and the establishment of a special data protection supervisory authority with strong enforcement powers are seen as essential, while in the United States, for example, there is no overarching privacy law but rather “a panoply of statutes” regulating different areas or practices, with different regulators with very different mandates and competences.⁹² In a number of countries, the areas listed in the chart may be regulated in different laws (rather than all being brought under one overarching national cybersecurity law) and be subject to different regulators. In this report, we will continue to focus on the global data protection frameworks and the roles of data protection authorities (while also noting the need for them to cooperate with other regulators).

4.2 The emerging global data protection framework

As noted in a recent UNCTAD report, there is:⁹³

“a lack of clarity and compatibility between regimes add uncertainty, with negative effects on investments; and ... given the nexus between cross-border e-commerce and data protection, divergent regimes will inhibit the adoption and proliferation of emerging technological developments, reducing potential accompanying societal benefits [but] Businesses are concerned that ... too stringent protection regimes will unduly restrict activities, increase administrative burdens and stifle innovation.”

To this should be added the crucial *caveat* that, not only in Europe but increasingly globally, important minimum requirements are increasingly firmly laid down in national constitutional and regional and global human rights- and consumer law: if those are deemed by other countries to be “too stringent” or “too high”, it will be impossible to avoid risks such as compulsory data localisation that could lead to the fragmentation of the Internet and the global digital world. The same applies to the denial to provide for equal privacy- and data protection for “everyone” in some countries.

However, as noted in Part 3, challenges remain in relation to the largely unanswered question of what kinds and depths of interferences should be allowed to protect national security, public security and cybersecurity; and in relation to the tension between encouraging free cross-border data flows to enhance trade and restrictions on such flows to protect privacy.

It is difficult to agree on the basic rules, expanding on the agreed basic principles in relation to the many different contexts to be covered (ranging from employment to health to communications and much beyond). It will be much more difficult to agree on the application of the permissible exceptions for national security, public security and cybersecurity – and on providing protection against abuses of those exceptions to “everyone”, including non-nationals. It is further likely that the issues relating to free trade and data protection will be equally difficult to resolve.

Still, at the international level, as noted in Part 2, there are signs of convergence in privacy- and data protection frameworks, and increased cooperation between relevant regulators, not least as concerns the development of rules and tools to allow international data transfers – *either* because they occur between countries that have effectively the same levels of protection, *or* because “appropriate safeguards” are provided by various means and mechanisms such as data transfer contracts, Binding Corporate Rules, sectoral Codes of Conduct, or privacy seals.

The OECD clearly encourages all relevant regulators in all OECD countries to cooperate with the EU authorities in this respect; and as we have seen, the Regulation in turn encourages the latter to reach out to regulators elsewhere.

However, again a similar *caveat* is required. The EU data protection authorities could be challenged if they were to agree to accept contracts, rules, codes or seals issued elsewhere, if those did not meet the constitutional (i.e., ECHR and EU Charter) requirements. Once again, therefore, the “Goldilocks Test” must in this particular context ensure compliance at least with the broad, fundamental global and human rights requirements. But provided that is done, they can be a major means of enabling a global data transfer regime pending the global adoption of statutory standards – provided, of course, that those standards are properly enforced.

4.3 Data protection regulators in practice

In Part 2 we noted that the Additional Protocol to the Data Protection Convention and, in particular, the EU GDPR set high standards for data protection authorities in terms of independence. The latter expressed this as follows:

<u>EU General Data Protection Regulation</u>	
Article 52	
<i>Independence [of data protection supervisory authorities]</i>	
1.	Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.
2.	The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.
3.	Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.
4.	Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.
5.	Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.
6.	Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

We also already noted in Part 2 that the GDPR requires that those independent DPAs be vested with extensive powers of enforcement⁹⁴ UNCTAD, adds that globally too:⁹⁵

Strong support exists for establishing a single central regulator when possible, with a combination of oversight and complaints management functions and powers. Moreover, the trend is towards broadening enforcement powers, as well as increasing the size and range of fines and sanctions in data protection.

This is reflected in the Model Laws. Thus, for instance, the HIPCAR Model Legislative Text stipulates that a Data Commissioner must be appointed, after consultation with both the Prime Minister and the Leader of the Opposition (S. 48); that that Commissioner must be independent in the exercise of his functions (S. 54) and may not be subjected to actions or proceedings in relation to acts done in good faith (S. 52); and that he must be vested with powers, *inter alia* to:

- control, inspect and verify processing operations;

- instruct data controllers “to take such measures as may be necessary to ensure that the processing of data is in accordance with [the data protection law]”;
- investigate complaints from data subjects and from “associations representing data subjects” and take (impose) “remedial action as the Data Commissioner deems necessary or as may be prescribed under this Act, and to inform the data subjects or associations of the outcome”; and
- collaborate with supervisory authorities of other countries to the extent necessary for the performance of his duties

(S. 55)

The EU data protection authorities have issued important, detailed guidance on the implementation of the EU rules, also in relation to the global digital environment, in particular through the so-called “Article 29 Working Party”, already mentioned, in which they closely cooperate (this is shortly to be replaced, under the new General Data Protection Regulation, with a European Data Protection Board, but that board will still be composed of representatives of the EU DPAs, and the European Data Protection Supervisor).⁹⁶

Again, such powers to issue guidance etc. are also envisaged in the Model Laws (cf. the HIPCAR Model Legislative Text, S. 55(f) and (j)).

However, it must be acknowledged that even in Europe DPAs have been less successful, and in some countries less willing, when it comes to actually enforcing the law and their interpretations of the law. This was made clear in a detailed comparative study of the authorities, commissioned by the EU’s Fundamental Rights Agency, and published in 2010.⁹⁷ However, as noted in Part 2, the new EU General Data Protection Regulation grants the authorities stronger powers – including the power to issue fines of up to 4% of a company’s annual turnover.

The FRA report also noted a “lack of data protection in the former third pillar of the EU” (police and judicial cooperation) – which is up to a point (but in the views of critics insufficiently) addressed in the recently adopted Law Enforcement Data Protection Regulation); and “a lack of clarity” regarding the extent of “broad exemptions and restrictions concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters), and the activities of the State in areas of criminal law” contained in the data protection directive. He added that:⁹⁸

In various Member States, these areas are altogether excluded from the protection of data protection law. This leaves a considerably large area unprotected with potentially serious consequences for fundamental rights protection.

That exclusion not only relates to the substance of the law (in the form of effectively or almost complete exemptions from the data protection requirements for the benefit of national security and other agencies); in many countries compliance with such data protection requirements as do apply is also not supervised by the normal DPA but by a special, usually less independent body, often with more limited powers than the normal DPA (e.g., in respect of access to the agencies’ files).

Both globally and in the supposedly (in data protection terms) most developed areas (Europe in particular), state surveillance is still lacking in real and effective systems of control, authorisation and supervision.⁹⁹

In other countries, supervision over compliance with data protection law may be split between different DPAs, e.g., different ones for the public and private sectors, or for different regions of the country. Although close coordination between such authorities in any one state is usually arranged for (e.g., in Germany, through the standing Conference of Data Protection Commissioners), such split authorities still add yet further complexity to an already complex area.

4.4 Other regulators

As noted earlier, the digital connected society may run on personal data, but the global digital environment is not only regulated by privacy and data protection laws – far from it. As the original explanatory memorandum to the OECD Guidelines already noted:¹⁰⁰

There are several international agreements on various aspects of telecommunications which, while facilitating relations and co-operation between countries, recognise the sovereign right of each country to regulate its own telecommunications (The International Telecommunications Convention of 1973). The protection of computer data and programmes has been investigated by, among others, the World Intellectual Property Organisation which has developed draft model provisions for national laws on the protection of computer software. Specialised agreements aiming at informational co-operation may be found in a number of areas, such as law enforcement, health services, statistics and judicial services (e.g. with regard to the taking of evidence).

In fact, there can be many different authorities with responsibilities in different fields that may have a part to play in the regulation of the digital environment, that may complement, and can sometimes overlap with, the roles of DPAs. For instance, telecommunication regulators are generally responsible for supervising the activities of telecommunication network- and service providers – and they have in several countries been assigned supervisory functions in relation to, e.g., the use of traffic- and location data generated in mobile communications (regulated in the EU in the e-Privacy Directive), or compulsory communication data retention such as was mandated by the EU Data Retention Directive (since declared invalid – although several EU Member States still retain the relevant legislation).

In the Netherlands, consumer protection authorities are charged with enforcement of the regulations on cookies and other forms of online tracking of individuals (another matter regulated in the EU in the e-Privacy Directive).

In other countries, especially those with mainly sectoral data protection/privacy laws (such as the US), there are often a wide range of quite different privacy regulators, each with special competence in a special field (e.g., health, finance, travel), and often with differing powers and differing degrees of independence.

Such diffusion of responsibilities may not be conducive to effective regulatory supervision, in particular in the area of a constitutionally-protected right such as data protection. Such other agencies – well-intended though they may be – are usually not equipped or specialised to deal with human rights issues or relevant technical matters; and may lack the degree of independence of special data protection authorities.

To foster efficiency and effective protection of data, data protection issues should be under the supervision of specialised data protection authorities – but those should then be enabled (in terms of status, powers, financing and technical facilities) to take effective enforcement

action; and its heads and staff should be appointed in a way that ensures they are committed to taking such action where appropriate.

NOTES:

¹ Ian Brown, *Working Paper No. 1: The challenges to European data protection laws and principles*, (Introduction, p. 1), produced as part of a major study for the European Commission led by Ian Brown and Douwe Korff, *New Challenges to Data Protection*, 2010. The Working Paper is available at:

http://ec.europa.eu/justice/data-protection/document/studies/files/new_privacy_challenges/final_report_working_paper_1_en.pdf

The *Working Paper* goes on to provide extensive further detail of the developments briefly noted here, to which the reader is referred.

² The Internet of Things is defined by the ITU as:

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

ITU-T Y.2060. For further discussion and references, see:

<http://www.itu.int/ITU-T/newslog/New+ITU+Standards+Define+The+Internet+Of+Things+And+Provide+The+Blueprints+For+Its+Development.aspx>

The OECD puts it as follows:

"The Internet of Things consists of a series of components of equal importance – machine-to-machine communication, cloud computing, big data analysis, and sensors and actuators. Their combination, however, engenders machine learning, remote control, and eventually autonomous machines and systems, which will learn to adapt and optimise themselves."

OECD (2015), *OECD Digital Economy Outlook 2015*, OECD Publishing, Paris, available at:

<http://dx.doi.org/10.1787/9789264232440-en>

³ See: Consumers International, *Connection and protection in the digital age: The Internet of Things and challenges for consumer protection*, April 2016, available at:

<http://www.consumersinternational.org/media/1657273/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf>

See also the accompanying Briefing, at:

<http://www.consumersinternational.org/media/1657279/briefing-connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf>

⁴ Douwe Korff, *The Rule of Law on the Internet and in the wider digital world*, *Issue Paper* published by the Council of Europe Commissioner for Human Rights, 2014, *Executive Summary*, pp. 7 – 8, available at: [https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CommDH/IssuePaper\(2014\)1&Language=lanAll&direct=true](https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CommDH/IssuePaper(2014)1&Language=lanAll&direct=true) (Choose language version)

⁵ ITU, *Trends in Telecommunication Reform 2016*, chapter 5, *Regulation and the Internet of Things*, Ian Brown, 2016.

⁶ See: Communication from the [EU] Commission to the Parliament, the Council etc., *A Digital Single Market for Europe*, *passim*, 6 May 2015 (COM(2015)192 final), available at:

<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN>

⁷ Accenture, *The Four Keys to Digital Trust*, 2014, available at:

https://acnprod.accenture.com/t20150709T093453_w_us-en/acnmedia/Accenture/Conversion-Assets/LandingPage/Documents/3/Accenture-3-LT-7-Four-Keys-Digital-Trust.pdf

⁸ On the differences between privacy in a narrow sense and data protection in the wider sense of protection against such misuses and abuses, see Part 2, section 2.2, below.

⁹ On the difference between targeted and indiscriminate ("generalised") data access by state authorities, see Part 3, below, in particular the discussion of the case-law of the Court of Justice of the EU.

¹⁰ See Douwe Korff, *The Rule of Law on the Internet and in the wider digital world* (note 4, above), Chapter 3: *The Rule of Law in the digital environment*.

¹¹ See: Consumers International, *Connection and protection in the digital age: The Internet of Things and challenges for consumer protection* (note 3, above), p. 40.

¹² See: EL Quinn, *Privacy and the New Energy Infrastructure*, SSRN Working Paper Series, 2009: <http://ssrn.com/abstract=1370731>

¹³ See: Douwe Korff and Marie Georges, *Passenger Name Records, data mining & data protection: the need for strong safeguards*, report for the Council of Europe Consultative Committee on data protection, June 2015, Council of Europe document T-PD(2015)11, section I.iii, *The dangers inherent in data mining and profiling*, available at:

[https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD\(2015\)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf](https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2015)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf)

¹⁴ See Samuel D. Warren and Louis D. Brandeis' famous essay, *The Right to Privacy*, Harvard Law Review, Volume IV, No. 5, December 15, 1890, available at:

<http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm>

¹⁵ ICCPR, Article 17 (privacy); ECHR, Article 8 ("private and family life"). Note that in spite of the different terminology in English, the terms were at least originally envisaged as meaning the same thing, as is clear from the use in the authentic French versions of both instruments of the term "*vie privée*". Note that the international human rights treaties protect individuals first and foremost against intrusions by states; protection against measures by other individuals or private entities such as companies is only accorded through indirect, so-called "horizontal application" of these treaty rights. The international remedies accorded under these treaties, too, can only be used *vis-à-vis* states, who can however be held accountable for not protecting individuals from interferences by others.

¹⁶ *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, Article 1 (author's translation).

The German Constitutional Court expanded on this in its famous *Census* judgment in 1983 as follows:

"A social and legal order in which the citizen can no longer know who knows what when about him and in which situation, is incompatible with the right to informational self-determination. A person who wonders whether unusual behaviour is noted each time and thereafter always kept on record, used or disseminated, will try not to come to attention in this way. A person who assumes, for instance, that participation in a meeting or citizen initiative is officially recorded, and may create risks for him, may well decide not to use the relevant fundamental rights ([as guaranteed in] Articles 8 and 9 of the [German] Constitution). This would not only limit the possibilities for personal development of the individual, but also the common good, because self-determination is an essential prerequisite for a free and democratic society that is based on the capacity and solidarity of its citizen."

Volkszählungsurteil, BVerfGE Bd. 65, S. 1 ff. (author's translation).

¹⁷ The ICCPR uses the words "without distinction" (Article 2(1)), where the ECHR uses "without discrimination" (Article 14), but the effect is identical.

¹⁸ The principle of universality of human rights was most clearly and simply, but emphatically, first expressed in the *Universal Declaration of Human Rights*, adopted by the U.N. General Assembly on 10 December 1948. The principle is also re-emphasised in the 1985 UN *Declaration on the Human Rights of Individuals who are not Nationals of the Country in which They Live*, although (as the title makes clear) this addresses the rights of people living in a state of which they are not a national rather than the rights of people affected by extraterritorially-applied laws and actions of states in which they do not live, but which affect them in the digital environment. For a more detailed discussion, see Douwe Korff, *The Rule of Law on the Internet and in the wider digital world* (note 2, above), Section 3.3, sub-section 3.3.1, *The principle of non-discrimination in international law*.

¹⁹ *Idem*, section 3.4, *"Within [a contracting state's] [territory and] jurisdiction"*, with extensive references to the relevant case-law.

²⁰ Such extraterritorial actions (or actions with effect in other countries) will also normally violate the sovereignty of the targeted state and thus be unlawful under public international law, see: Douwe Korff, *Expert Opinion*, prepared for the Committee of Inquiry of the German *Bundestag* into the "5EYES" global surveillance systems revealed by Edward Snowden, presented at the Committee Hearing, Berlin, 5 June 2014, available at: http://www.bundestag.de/blob/282874/8f5bae2c8f01cdabd37c746f98509253/mat_a_sv-4-3_korff-pdf-data.pdf (full text in English, in spite of what it says on the cover page):

http://www.bundestag.de/blob/282876/b90dd97242f605aa69a39d563f9532e7/mat_a_sv-4-3_korff_zusammenfassung-pdf-data.pdf (summary in English)

However, this is not further discussed in this paper.

²¹ See note 15, above.

²² See Douwe Korff, *The Rule of Law on the Internet and in the wider digital world* (note 4, above), Section 3.4, *"Within [a contracting state's] [territory and] jurisdiction"*, under the heading "The US Government and the ICCPR".

²³ The quotes are from the second preamble to the 1995 EC Data Protection Directive, further discussed in sub-section 2.4.3.

²⁴ *Idem*, seventh preamble. The text there refers to data flows between EU Member States and obstacles to intra-EU trade etc., but the dilemma of course arises equally in other regions and trading zones, and at a wider, global level.

²⁵ OECD, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980, available at: <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>

²⁶ See: <https://www.oecd.org/sti/ieconomy/privacy.htm>

Chapter 4, *The evolving privacy landscape: 30 years after the OECD Privacy Guidelines (2011)* provides a very useful oversight of the historical developments on privacy generally.

²⁷ United Nations, Guidelines for the Regulation of Computerized Personal Data Files, UNGA Res. 44/132, 44 UN GAOR Supp. (No. 49) at 211, UN Doc. A/44/49 (1989), available at: <https://www1.umn.edu/humanrts/instrree/q2grcpd.htm>

²⁸ Available at: http://publications.apec.org/publication-detail.php?pub_id=390

²⁹ Available at:

<http://www.apec.org/~media/Files/Groups/ECSG/CBPR/CBPR-CrossBorderPrivacyEnforcement.pdf>

³⁰ See the OECD Guidelines, Part Two (“Basic Principles of National Application”); UN Guidelines, Section A (“Principles concerning the Minimum Guarantees that should be provided in National Legislation”); APEC Privacy Framework, Part III (“APEC Information Privacy Principles”).

³¹ Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature in Strasbourg on 28 January 1981, CETS No. 108, available at: <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>

³² Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, opened for signature in Strasbourg on 8 November 2001, CETS No. 181, available at:

<https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680080626>

The Additional Protocol was to a large extent aimed at bringing the Convention in line with the EU rules on the added matters (discussed later in the text), which were not or insufficiently addressed in the original Convention.

³³ Within the Council of Europe, data protection issues are further addressed by a number of bodies including the Parliamentary Assembly of the Council of Europe (PACE), a Consultative Committee, known as “T-PD”, established by Convention No. 108, and the Council of Europe Committee of Ministers (COM or CM). Between them, they have issued many opinions, recommendations and studies in the area – always with reference to the Convention. See:

http://website-pace.net/en_GB/web/apce/documents (PACE documents) Note that these cover many more issues than just data protection – but they can be searched under the term “data protection”. On 14 April 2016 this provided 265 results.

https://www.coe.int/t/dghl/standardsetting/dataprotection/Documents_TPD_en.asp (T-PD documents);

https://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp (COM documents relating to data protection).

In addition, there is an interplay between the Data Protection Convention and the European Convention on Human Rights, with the European Court of Human Rights increasingly taking note of the Data Protection Convention and the above-mentioned kinds of documents in its own interpretation of Article 8 of the Human Rights Convention (which guarantees the right to private life); while PACE, the Consultative Committee and the Committee of Ministers in turn draw on the case-law of the Court in their work in this area. See the ECtHR Factsheet – personal data protection (note 16, above) and *Annex 1 – Jurisprudence* to a recent working document by the EU’s “Article 29 Working Party”, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) (note 41, below), which lists 15 important ECtHR judgments relevant to data protection (and five CJEU ones).

³⁴ Council of Europe Ad hoc Committee on Data Protection (CAHDATA), Working Document containing the Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), available at:

https://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/Draft%20amending%20protocole%20with%20reservations_En.pdf

³⁵ Full title: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995, pp. 0031 – 0050, available at:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

³⁶ Full title: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201, 31/07/2002, pp. 0037 – 0047, available at:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML>

In 2006, a further directive, known as the Data Retention Directive, was adopted, technically in the form of an amendment to the e-Privacy Directive, that required the compulsory retention of electronic communications data beyond the period for which those data would normally be retained by the relevant e-communications companies for their own business purposes, so that those data could be accessed and analysed by Member States' authorities "for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law". Full title: Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105, 13/04/2006, pp. 0054 – 0063, available at:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>

However, in 2014, in the *Digital Ireland* case (Joined Cases C-293/12 and C-594/12) the Court of Justice of the EU ruled that this directive was invalid because it did not meet the requirements of the European Union's Charter of Fundamental Rights (see Part 3, below). This Charter had become binding law within the Union by virtue of the Lisbon Treaty which entered into force in 2009. It guarantees both a general right to respect for private and family life, on the lines of the corresponding right in the ECHR (Article 7 CFR), but also the new, special *sui generis* right to data protection as developed in the EU Member States (as discussed at 2.1, above) (Article 8 CFR).

³⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal L 119, 04/05/2016, pp. 0001 – 00149, available at:

<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN>

³⁸ See:

<https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive>

³⁹ A fourth issue, the question of (extra-)territorial jurisdiction, is discussed separately in sub-section 2.4.5.

⁴⁰ For brief summaries of the ECtHR case-law, see the Court's Factsheet – personal data protection (note 16, above). The Article 29 Working Party has analysed the requirements that flow from the EU directives and the EU Charter of Fundamental Rights as interpreted in the case-law of the Court of Justice of the EU and of the European Court of Human Rights in a very recent, more extensive and thorough working document on surveillance, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) (WP237), adopted on 13 April 2016, available at:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf

Annex 1 – Jurisprudence to this document lists 15 important ECtHR judgments relevant to data protection: *Klass and others v. Germany*, 6 September 1978, Application no. 5029/71; *Malone v. United Kingdom*, 2 August 1984, Application no. 8691/79; *Leander v. Sweden*, 26 March 1987, Application no. 9248/81; *Huvig v. France*, 24 April 1990, Application no. 11105/84; *Hokkanen v. Finland*, 23 September 1994, Application no. 19823/92; *López Ostra v. Spain*, 9 December 1994, Application no. 16798/90; *Chahal v. United Kingdom*, 15 November 1996, Application no. 22414/93; *Amman v. Switzerland*, 16 February 2000, Application no. 27798/95; *Rotaru v. Romania*, 4 May 2000, Application no. 28341/95; *Copland v. United Kingdom*, 3 April 2007, Application no. 62617/00; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, 28 June 2007, Application no. 62540/00; *Liberty and others v. United Kingdom*, 1 July 2008, Application no. 58243/00; *S. and Marper v. United Kingdom*, 4 December 2008, Applications nos. 30562/04 and 30566/04; *Gillan and Quinton v. United Kingdom*, 12 January 2010, Application no. 4158/05; *Bucur and Toma v. Romania*, 8 January 2013, Application no. 40238/02. All these can be found on the ECtHR's case-law (HUDOC) website:

<http://hudoc.echr.coe.int/eng>

It also lists five CJEU judgments (including two already mentioned): *Commission v. Germany*, 9 March 2010, Case C-518/07; *Commission v. Austria*, 16 October 2012, Case C-614/10; *Commission v. Hungary*, 8 April 2014, Case C-288/12; *Digital Rights Ireland*, 8 April 2014, Joined Cases C-293/12 and C-594/12 (note 35, above); *Schrems v. Data Protection Commissioner of Ireland*, 6 October 2015, Case C-362/14 (note 41, above). All these can be found on the CJEU's case-law (CURIA) website:

http://curia.europa.eu/jcms/jcms/j_6/

⁴¹ *Schrems v. Data Protection Commissioner of Ireland* (note 41, above), paras. 93 and 94. The Council of Europe Convention also refers to "equivalent protection" but in more ambiguous terms: see Article 12(3)(a)).

⁴² *Idem*, para. 74.

⁴³ Cf. *idem*, para. 94; see also the Article 29 Working Party Working Document 01/2016 (note 47, above) and the Legal Opinion of the European Parliament's legal service (note 46, above).

⁴⁴ Such "generalised access" to communications content was held by the CJEU to infringe the very "essence" of the right to data protection: *Schrems v. Data Protection Commissioner of Ireland* (note 41, above), para. 73.

⁴⁵ Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (note 34, above), Article 14 (previously Article 12), para. (1), added second sentence.

⁴⁶ GDPR, Article 46 (which must be read with the more detailed rules on the means mentioned and the stipulations on the powers of the authorities relating to these means and mechanisms).

⁴⁷ Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (note 34, above), Article 14(new)(3)(b), which stipulates that "[an appropriate level of protection can be secured by] ... ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing."

⁴⁸ *Re* the Council of Europe, see note 33, above. For the EU, the 1995 Data Protection Directive established a body, somewhat prosaically referred to as "the Article 29 Working Party" after the article establishing it, which brings together representatives of all the data protection authorities in the EU and the EEA. It issues numerous opinions and working documents which, while not formally binding, are highly authoritative in terms of the interpretation and application of EU data protection law, and taken into account inter alia by the EU Court of Justice in its rulings on relevant matters. The Article 29 Working Party (WP29) opinions and working documents etc. can be found here:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

WP29 documents relevant to the global digital environment include (in reverse chronological order, from 2010 only): 2016: an opinion on the proposed EU-US Privacy Shield (WP238); a working document on privacy and data protection and surveillance (WP238), which followed on from an earlier working document (WP228) and opinion (WP215); 2015: an opinion on the question of applicable law in the digital environment, in the light of the CJEU *Google Spain* ("right to be forgotten") judgment (WP179 update), which followed on from earlier guidelines (WP225); a statement on the implementation of the *Schrems* judgment (no number); an opinion on the C-SIG Code of Conduct on Cloud Computing (WP232); an report on a "cookie sweep combined analysis" (WP229); 2014: an opinion on the application of the e-Privacy Directive to device fingerprinting (WP224); an opinion on "recent developments on the Internet of Things (WP223); a statement on the implications of the *Digital Rights Ireland* case (WP220); 2013: an opinion on obtaining consent for cookies (WP208); an opinion on apps on smart devices (WP202); 2012: an opinion on cloud computing (WP196); an opinion on cookie consent exemption (WP194); 2011: an opinion on geolocation services on smart mobile devices (WP185); 2010: an opinion on global transfers of passenger name record (PNR) data to third [i.e., non-EU/EEA] countries; etcetera.

Also important are the opinions of the European Data Protection Supervisor, which can relate to all areas of Union, i.e., both to matters addressed in the EC directives and in the instruments relating to police and judicial cooperation. They can be found here:

<https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Publications>

⁴⁹ See in particular cases C-518/07 of 9 March 2010 against Germany, C-614/10 of 16 October 2012 against Austria, and C-288/12 against Hungary.

⁵⁰ See GDPR, Chapter VI, Independent Supervisory Authorities, section 1, *Independent Status*, in particular Article 52.

⁵¹ *Idem*, Article 57.

⁵² *Idem*, Article 58 (selection). The article lists altogether 6 "investigative powers", 10 "corrective powers", and 10 "authorisation and advisory powers"; and adds to this a power "to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal

proceedings, in order to enforce the provisions of this Regulation". The EU Member States may add even further powers to all this.

⁵³ Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (note 34, above), Article 15, moving Article 1 of the Additional Protocol into the main text. On the required powers of the authorities, see in particular Article 15(2) and (4).

⁵⁴ Establishment of Harmonized Policies for the ICT Market in the ACP Countries, HIPCAR, Privacy and Data Protection: Model Policy Guidelines & Legislative Texts, ITU 2012, available at: http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Documents/FINAL%20DOCUMENTS/ENGLISH%20DOCS/privacy_and_data_protection_model%20policy%20guidelines.pdf

⁵⁵ Establishment of Harmonized Policies for the ICT Market in the ACP Countries, HIPSSA, Data Protection: Southern African Development Community (SADC) Model Law, ITU 2013, available at: http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

⁵⁶ Projets de Lois Types de la Communauté Economique des Etats de l'Afrique Centrale (CEEAC) et Projets de Directives de la Communauté Economique et Monétaire de l'Afrique Centrale (CEMAC), Cybersécurité, ITU 2013, available (in French only) at: http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/REGIONAL%20documents/projets_des_lois_types-directives_cybersecurite_CEEAC_CEMAC.pdf

⁵⁷ Cf. HIPCAR, Privacy and Data Protection: Model Policy Guidelines & Legislative Texts (note 53, above), Article 19(1) ("comparable level of protection"); HIPSSA, Data Protection: Southern African Development Community (SADC) Model Law (note 54, above), Article 44 ("adequate"); CEEAC/CEMAC Model Law/Directive on Data Protection (note 55, above), Article 60 ("adequate").

⁵⁸ See Douwe Korff, The Rule of Law on the Internet and in the wider digital world (note 4, above), section 3.6, *Exercise of extraterritorial jurisdiction by states*, with detailed references. See also the discussion of the ECtHR *Perrin* case and the French *Yahoo!* case in Douwe Korff & Ian Brown, *Social media and human rights*, Chapter 6 in: Human rights and a changing media landscape, Council of Europe, 2011, p. 195ff., available at: <https://www.coe.int/t/commissioner/source/prems/MediaLandscape2011.pdf>.

See also more generally the Internet & Jurisdiction Project:

<http://www.internetjurisdiction.net/>

And more specifically: Bertrand de La Chapelle and Paul Fehlinger, Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation, available at:

<http://www.internetjurisdiction.net/wp-content/uploads/2016/04/Internet-Jurisdiction-Project-Jurisdiction-on-the-Internet-by-Bertrand-de-La-Chapelle-and-Paul-Fehlinger.-Global-Commission-on-Internet-Governance.pdf>

⁵⁹ Scassa, Teresa and Robert J. Currie, New First Principles: Assessing the Internet's Challenges to Jurisdiction, Georgetown Journal of International Law 42(4): 1018 (2010), quoted in Bertrand de La Chapelle and Paul Fehlinger, Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation (previous note), Executive Summary.

⁶⁰ *Google Spain v. AEPD*, Case C-131/12, CJEU Grand Chamber judgment of 13 May 2014, para. 60 (where the Court applied this approach specifically to search engines and establishments linked to search engines). See also the Article 29 Working Party Opinion on the question of applicable law in the digital environment, in the light of the CJEU Google ("right to be forgotten") judgment (WP225). For a further discussion, see: Brendan Van Alsenoy and Marieke Koekoek, Internet and Jurisdiction after Google Spain: The Extraterritorial Reach of the EU's "Right To Be Forgotten", 2015, available at: https://ghum.kuleuven.be/ggs/publications/working_papers/new_series/wp151-160/wp152-alsenoy-koekoek.pdf

⁶¹ The English version of the Directive uses the word "equipment", but other language versions – which in EU law are equally authentic – use the relevant word for "means", such as "*moyens*" (French), "*Mittel*" (German).

⁶² Article 29 Working Party, Opinion 8/2010 on applicable law, adopted on 16 December 2010 (WP179), pp. 20 – 22.

⁶³ See Douwe Korff, Expert Opinion, prepared for the Committee of Inquiry of the German *Bundestag* into the "5EYES" global surveillance systems revealed by Edward Snowden (note 20, above), section A.2, p. 4ff.

⁶⁴ See Douwe Korff, *The Rule of Law on the Internet and in the wider digital world* (note 4, above), section 4.5.5, *Investigating crimes in the digital environment*, under the heading “Article 32 of the Cybercrime Convention”.

⁶⁵ See: David Banisar (of the NGO Article 19), *National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map*, available at:

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416

Also: DLA Piper, *Data Protection Handbook*, providing basic information on countries with privacy laws worldwide and also including a world map:

<https://www.dlapiperdataprotection.com/#handbook/>

https://www.dlapiperdataprotection.com/#handbook/world-map-section/c1_HK/c2_GB

⁶⁶ United Nations Conference on Trade and Development (UNCTAD), *Data protection regulations and international data flows: Implications for trade and development*, 2016, Executive Summary, p. 7, available at:

http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_summary_en.pdf

The full report is available here:

http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_summary_en.pdf

⁶⁷ Turkey was the last Council of Europe Member State to ratify the Convention, which it did on 2 May 2016. The Convention will enter into force for Turkey on 1 September 2016.

⁶⁸ UN GA Resolution 68/167 on the right to privacy in the digital age, adopted on 18 December 2013, UN Document A/RES/68/167, available at:

http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167

⁶⁹ Report of the High Commissioner for Human Rights on the right to privacy in the digital age, UN Document A/HRC/27/37, 30 June 2014, available from:

http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

For more general information on the UN developments, see:

<http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx>

⁷⁰ The Special Rapporteur on the Right to Privacy presented his first report to the Human Rights Council in March 2016, which set out detailed plans to address the issues at the global level, see: *Report of the Special Rapporteur on the right to privacy*, Joseph A. Cannataci, UN Document A/HRC/31/64, 8 March 2016, available from:

<http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>

⁷¹ *Supplementary Explanatory Memorandum to the Revised OECD Privacy Guidelines*, section on *Transborder flows of personal data*, p. 30.

⁷² See the Article 29 Working Party documents on biometrics: WP29 *Working document on biometrics* (WP80, 2003); WP29 *Opinion 02/2012 on facial recognition in online and mobile services* (WP192); WP29 *Opinion 3/2012 on developments in biometric technologies* (WP193), all available from:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/index_en.htm

⁷³ See: *UN Guidelines*, Principle 6; *OECD Guidelines*, Principle 4; *APEC Privacy Framework*, Principle 13; Council of Europe *Data Protection Convention*, Article 8; EU *Data Protection Directive*, Article 13; EU *General Data Protection Regulation*, Article 23.

⁷⁴ See: Douwe Korff, Ben Wagner, Julia Powles and others, *Boundaries of Law: exploring transparency, accountability and oversight of government surveillance regimes* (forthcoming).

⁷⁵ *Idem*.

⁷⁶ See the selection of “cybersecurity” definitions in this handout and presentation:

<https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CPDP%202015%20-%20KORFF%20Handout%20-%20DK150119.pdf>

<https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CPDP%202015%20-%20KORFF%20presentation.pdf>

The ITU defines cybersecurity as “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets.” See:

<http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx>

⁷⁷ Note that the Council of Europe *Cybercrime Convention* (also known as the “Budapest Convention”), which lists many specific “cybercrimes”, still leaves the states that are party to it considerable leeway in the definition of those crimes, including the exceptions to those crimes (e.g., in relation to intellectual property issues and hate crimes).

⁷⁸ But note that in reality, data in “cyberspace” are still always in some country. This is further discussed later in the text in relation to cross-border law enforcement and national security activities.

⁷⁹ See note 13, above.

⁸⁰ Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, and Daniel J. Weitzner, Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications, Computer Science and Artificial Intelligence Laboratory Technical Report, Massachusetts Institute of Technology, MIT-CSAIL-TR-2015-026, 6 July 2015, available at: <https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf>

The quoted text is from the Executive Summary.

⁸¹ See again the paper and Executive Summary mentioned in the previous note. Also the European Digital Rights (EDRI), Position paper on encryption: High-grade encryption is essential for our economy and our democratic freedoms (prepared by EDRI member organisation Bits of Freedom), 7 January 2016, available at: <https://www.edri.org/files/20160125-edri-crypto-position-paper.pdf>

⁸² See, with particular reference to the issues in the Cybercrime Convention, Douwe Korff, The Rule of Law on the Internet and in the wider digital world (note 4, above), Section 4.5.5, “*Investigating crimes in the digital environment*”.

⁸³ On the Reference Guide, see:

<http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx>

As explained there, the Reference Guide is being developed in a project carried out by the ITU in partnership with the CCI, CTO, ENISA, GCSP, GCCC University of Oxford, Microsoft, NATO CCDCOE, OECD, OAS, UNCTAD and World Bank.

The National Cyber Security Strategy (NCS) Toolkit can be found here:

<http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf>

⁸⁴ See:

<http://www.oxfordmartin.ox.ac.uk/cybersecurity/>

⁸⁵ See:

<http://www.thegfce.com/>

⁸⁶ The starting point for the latter could be the “*intelligence codex’ addressed to the intelligence services of all [Council of Europe Member States], which lays down rules governing co-operation in the fight against terrorism and organised crime*”, recommended by the Parliamentary Assembly of the Council of Europe (PACE) in its Recommendation on Mass Surveillance, Recommendation 2067 (2015), 21 April 2015, para. 2.3, available at:

<http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=21694&lang=en>

However, rather than only addressing “co-operation”, it should also set standards and limitations on what the agencies may and may not do, even purely domestically. That could be done indirectly, by such a “codex” stipulating that state agencies should not co-operate with agencies of other states unless those other agencies were subject to such standards and limitations – but it would be better stipulated directly.

⁸⁷ See: http://ec.europa.eu/trade/policy/in-focus/ttip/index_en.htm

⁸⁸ See: http://ec.europa.eu/trade/policy/in-focus/ceta/index_en.htm

⁸⁹ See: <https://ustr.gov/tpp/>

⁹⁰ For an overview of the criticisms, in particular in relation to digital rights (including not just data protection but also copyright and net neutrality, etc.), see the EDRI booklet, TTIP and digital rights, available at: https://edri.org/files/TTIP_and_DigitalRights_booklet_WEB.pdf

⁹¹ ITU data, 2015.

⁹² For an overview, see Chris Hoofnagle, *Country Study – United States of America*, produced as part of a major study for the European Commission, New Challenges to Data Protection, 2010, available at:

http://ec.europa.eu/justice/data-protection/document/studies/files/new_privacy_challenges/final_report_country_report_b1_usa.pdf

⁹³ UNCTAD, Data protection regulations and international data flows: Implications for trade and development, 2016, Executive Summary (note 66, above), p. 7. Point re-ordered.

⁹⁴ See the list of powers that must be granted to the data protection authorities under the GDPR, summarised in Part 2, at the end of sub-section 2.4.3.

⁹⁵ UNCTAD, Data protection regulations and international data flows: Implications for trade and development (note 66, above), Executive Summary, p. 7.

⁹⁶ On the Article 29 Working Party and these recommendations etc., see note 48, above. On the new EDPB, see the GDPR, Chapter VII, Section 3, Articles 68 – 76. The Board’s independence is addressed in Article 69.

⁹⁷ EU Fundamental Rights Agency, Data Protection in the European Union: the role of National Data Protection Authorities (a second report by the FRA on “Strengthening the fundamental rights architecture in the EU”), 2010, available at:

http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf

⁹⁸ *Idem*, Executive Summary, p. 7.

⁹⁹ See Douwe Korff, Ben Wagner, Julia Powles and others, Boundaries of Law: exploring transparency, accountability and oversight of government surveillance regimes (note 74, above), section 2.3.3, *Untargeted generic access (“mass surveillance”)*, at (d) Formal requirements and (f), Oversight.

¹⁰⁰ Original Explanatory Memorandum to the OECD Privacy Guidelines (1983), p. 43.

- o - O - o -