BUILDING TRUST TO PROMOTE REGULATORY CO-OPERATION AND COHERENCE

05

This chapter provides an overview of the role that regulatory co-operation can play in supporting the development of the digital economy within Commonwealth member countries. The first section discusses the synergies between data regulations, Open Government Data, e-commerce and digital trust. It also describes the existing models for data protection and flows, and the potential scope for the Commonwealth to collaborate in these areas. The second section maps out the need to update the taxation policies of Commonwealth countries to adapt to the changing economic landscape in the digital age. The third section explores issues of competition and intellectual property laws in the digital era.

5.1 Regulatory practices and digital trust

To manage the rapid progress of digital technologies in a more inclusive manner, there is a need for evolution of the ICT regulatory environment, in terms of legal and regulatory frameworks as well as the quality of ICT regulations and the coherence of these regulations across different levels. Regulations can be applied at the: a) national level – for instance, the introduction of a national law in a country; b) regional level, as in the European General Data Protection Regulation (GDPR); and c) international level – governed by bilateral or multilateral trade agreements such as those at the WTO.

The ITU has developed an ICT Regulatory Tracker that identifies trends in ICT legal and regulatory frameworks. While it does not measure the quality or the level of implementation or performance of regulatory frameworks, it helps progress and identify gaps in **national regulatory frameworks** using four dimensions: **regulatory authority, regulatory mandate, regulatory regime and competition framework**. The regulatory authority dimension includes indicators measuring, for example, the presence of a separate ICT regulator, autonomy of the regulator in decision-making, accountability, enforcement power, dispute resolution and the presence of a competition authority. Regulatory mandate examines who has control in the country for regulating the following: licensing, quality of service obligations measures, radio frequency allocation, universal access, broadcasting and internet content. In turn, regulatory regime captures the existence of regulations in major areas, including types of licensing, use of Voice over Internet Protocol (VoIP) services, mandated infrastructure sharing and co-location, and presence of a national plan that involves broadband. Lastly, the competition framework measures the level of competition in the main market segments within the ICT sector, i.e. existence of competition in local and long distance fixed line services; 3G, 4G and other services, as well as foreign ownership or participation in facilities-based operators; spectrum-based operators; local service operators/long-distance service operators; international service operators; and ISPs.

Using this ICT Regulatory Tracker, Table 5.1 compares Commonwealth countries across the four different dimensions. It is observed that Malta, the UK and Australia rank in the top ten countries out of 193 countries globally. Within the Commonwealth, small states are performing least favourably in terms of ICT regulations, and the regulatory authority and regulatory regime dimensions.

In addition to putting in place appropriate ICT regulations – such as those related to ICT access, barriers to entry and exit in the communications sectors, foreign participation in internet services provision, privacy and data protection, and mergers – it is also necessary for them to be coherent and complementary across national and international levels. At the national level, better and targeted dialogue is needed among the government, private sector players and educational institutions in order to understand the challenges facing industrialisation and find innovative solutions to address them.

Rwanda, with its aim to create a comprehensive legal framework for regulating ICT activities, serves as a good example among developing Commonwealth member states – Rwanda's score on the regulatory authority and regulatory mandate indicators in Table 5.1 is the same as that of the UK. Since 2006,

Table 5.1 Ranking of Commonwealth countries on ITU's ICT regulatory Tracker

Name	Regulatory authority	Reg. mandate	Reg. regime	Competition framework	Rank
Malta	19	20	28	28	5
United Kingdom	20	20	28	27	5
Australia	19	21.5	26	28	8
Singapore	17	21.5	26	27	26
Bahamas, The	19	18.5	26	25.33	35
Ghana	18	21	22	27	42
Pakistan	20	19	22	27	42
Kenya	18	21.5	21	27	45
Malawi	18	22	20	27	47
Malaysia	18	22	24	23	47
Uganda	17	20	22	27	52
Cyprus	18	16	28	23.67	57
Canada	19	16.5	30	20	58
Trinidad and Tobago	18	19	22	26.33	61
Botswana	18	22	19	26	62
Saint Lucia	16	18	24	27	62
Tanzania	20	21	19	25	62
Rwanda	20	20	18	24.33	73
Mauritius	18	20.5	15	27.33	81
New Zealand	17	13.5	22	28	83
Saint Vincent and the Grenadines	17	18	18	27	85
Jamaica	19	12.5	19	28	90
Nigeria	17	20	20	21.33	91
India	18	14.5	20	23	94
Bangladesh	17	20	15	22.67	96
Grenada	14	17	20	23	99
Gambia, The	20	19	16	18.67	103
Dominica	11	15.5	20	26	106
Zambia	19	18	15	19.67	109
South Africa	17	17	24	13.33	112
Vanuatu	17	14.5	14	25.67	114
Namibia	19	17	22	12.67	116
Barbados	17	12.5	18	21	123

(*Continued*)

Table 5.1 Ranking of Commonwealth countries on ITU's ICT regulatory Tracker (*Continued*)

Name	Regulatory authority	Reg. mandate	Reg. regime	Competition framework	Rank
Lesotho	16	17.5	16	18.33	126
Samoa	14	17	22	13.33	130
Cameroon	17	18	16	13	135
Fiji	13	14	19	17	138
Belize	17	18.5	20	7.33	141
Sri Lanka	18	20	15	9.33	142
Guyana	18	18	15	11	143
Seychelles	6	12	16	28	143
Brunei Darussalam	15	17	17	12.33	148
Eswatini	19	19	14	7.33	150
Papua New Guinea	16	19.5	12	11	151
Mozambique	16	10.5	16	15.17	156
Sierra Leone	16	19	14	7	157
Nauru	10	11.5	6	23	163
Tonga	1	11	15	22.67	165
Kiribati	13	18.5	4	12	167
Saint Kitts and Nevis	5	15	6	20	168
Antigua and Barbuda	8	11.5	8	13.33	174
Solomon Islands	9	14	8	3.67	177
Tuvalu	0	4.5	0	5	189

Source: ITU (2018b).

government efforts have been directed towards privatisation of state-owned enterprises to reduce the government's non-controlling share in private firms and to attract FDI, particularly in ICT services (US Department of State 2019). In 2016, the Rwandan government adopted the ICT Act, which institutes an ICT regulatory authority responsible for implementing the country's international obligations in ICT, as well as promoting fair competition in the sector, and applies to all electronic communications, information society, and the broadcasting and postal sectors.

Data regulations, which are separate from regulations in the ICT sector, are becoming increasingly important to foster online consumer trust in the digital economy. Historically, national data protection authorities have monitored issues relating to privacy and regulated the use of data through privacy and data protection laws, cybercrime legislation, rules pertaining to privacy and sharing of specific types of data (e.g., health or financial data), and now rules about electronic transactions (ITU 2018b). Currently, 74 countries across the world have established a separate data protection regulator, while in 63 countries data protection is under the broad mandate of the ICT regulator, including in Commonwealth countries such as Rwanda and Saint Kitts and

Nevis. However, Chapter 2 showed that the majority of the Commonwealth countries with legislation in only one of the four data legislation areas – a) electronic transactions/e-signature; b) data protection/privacy online; c) consumer protection when purchasing online; and d) cyber-crime prevention – are African countries (such as Mozambique, Lesotho, Nigeria, Tanzania and Malawi) and small states such as PNG, Solomon Islands and Vanuatu. This poses questions about how active a role the ICT regulatory authority is playing in regulating data in these Commonwealth countries. See Box 5.1 for a case-study on ICT regulations in Kenya.

The development of a comprehensive legal and regulatory framework on data can in fact be the key to unlocking digital trust for e-commerce in many developing Commonwealth countries. CIGI-Ipsos (2017) conducted a survey of 24,225 internet users in 24 countries, including the Commonwealth countries of Australia, Canada, Kenya, India, Nigeria, Pakistan, South Africa and the UK, and found that 49 per cent of the those

Box 5.1 ICT regulations in Kenya

A key challenge to digital transformation in Kenya is poor management of ICT regulations. Regulations for the ICT services sector are spread out between the central government and state entities in Kenyan counties, leading to unclear division of responsibilities and overlapping roles (Waema and N'dungu 2012), and resulting in higher transaction (compliance) costs for private players. Fragmentation makes it more difficult: a) for regulatory institutions to prosecute cybercrime such as software piracy, which deters foreign investment; and b) to fully align regulations with international standards. Kenya does not currently have a national data protection authority. However, there is draft legislation in the Senate, the Data Protection Bill 2018, that aims to establish such an authority. This bill bears some similarities to the UK's Data Protection Act 2018, which incorporates and supplements the provisions of the GDPR. It embraces the basic principles of data protection: the necessity of collecting information, the right of subjects to access information, imposition of duty to ensure that the information is updated, complete and correct (Okal 2017). In addition, Section 31 of the bill prohibits the transfer of personal data out of Kenya unless: the third party is subject to a law or agreement that requires putting in place adequate measures for the protection of personal data; that the data subject consents to the transfer; that the transfer is necessary for the performance or conclusion of a contract between the agency and the third party; or that the transfer is for the benefit of the data subject.

Kenya launched the National ICT Master Plan in 2017 to harness the power of ICT, increasing Kenya's regional and global competitiveness. To prevent copyright and digital content piracy, the Kenya Copyright Board is working on the Copyright Amendment Bill 2016 (Okal 2017). This bill will facilitate protection of creative works on online platforms, enabling greater digital trade. Moreover, Kenya launched the Cyber Security and Protection Bill in 2016 to provide increased security in cyberspace, enabling greater information sharing, protection of life and national security (Okal 2017).

Source: Authors, Ogletree Deakins (2019).

who never shopped online cited a lack of trust as the primary obstacle. Among those worried about their privacy, top sources of concern included cybercrime (82%), internet companies (74%) and governments (65%) (CIGI 2017). The survey further provides some country-level insights into the importance of different regulations or protection in determining engagement in online shopping, which are outlined in Table 5.2. In an e-trade assessment for LDCs, UNCTAD (2019) confirms that lack of trust is a critical barrier to the uptake of e-commerce payments – low levels of digital trust prevent consumers from moving from cash on delivery towards e-payments.

Updating e-commerce legislation and regulations, including in the field of data privacy, consumer protection, cyber-law and dispute resolution can build online consumer trust and facilitate inclusion of developing Commonwealth countries in digital trade. Models for data protection, however, vary and can be tailored to the nature of the local market (CIPE 2018). For instance, some economies such as those in the EU and Ghana have adopted more comprehensive over-arching regulations on open data protection, while others have implemented sector-specific laws. Within consumer protection, CIPE (2018) highlights dispute resolution as a key area to be addressed. Dispute resolution is crucial for enterprises and consumers alike, given that merchant-customer disputes frequently arise in electronic transactions at the post-sale phase. To streamline enforcement, governments and businesses alike are increasingly turning to alternative means of dispute resolution, especially online dispute resolution (ibid).

Within data regulations, cross-border flows of data, source-code sharing, and data localisation are contentious issues between Commonwealth countries. One of the channels through which free flow of data is operationalised is through no requirements of data localisation i.e. foreign firms collecting data from a country have the freedom to move it across the border and store it in any part of the world. The decision to locate data centres by global private sector players can be based on cost-efficiencies, geographical reasons, legal frameworks and political factors (Meltzer 2015). On the one hand, forced data localisation may increase economic costs (Bauer et al. 2014); but on the other hand, many developing countries see data localisation measures as the exercise of national sovereignty and protection of their consumer data, which can strengthen the position of domestic firms and local digital ecosystems, enabling catch-up (Azmeh et al. 2019; UNCTAD 2018).

Table 5.2 Percentage of internet users considering regulations 'important' for e-commerce engagement

Country	Online consumer protection	Data privacy	Protection against data breaches	Protection against cyber-crime	Online or offline cross-border dispute resolution mechanisms
Kenya	99	99	96	98	94
Nigeria	90	87	88	87	86
South Africa	96	96	95	95	90
India	97	92	91	92	88
Canada	97	97	96	96	88
Australia	94	95	94	95	87
Global (24 countries)	94	94	93	94	87

Source: CIGI-Ipsos (2017).

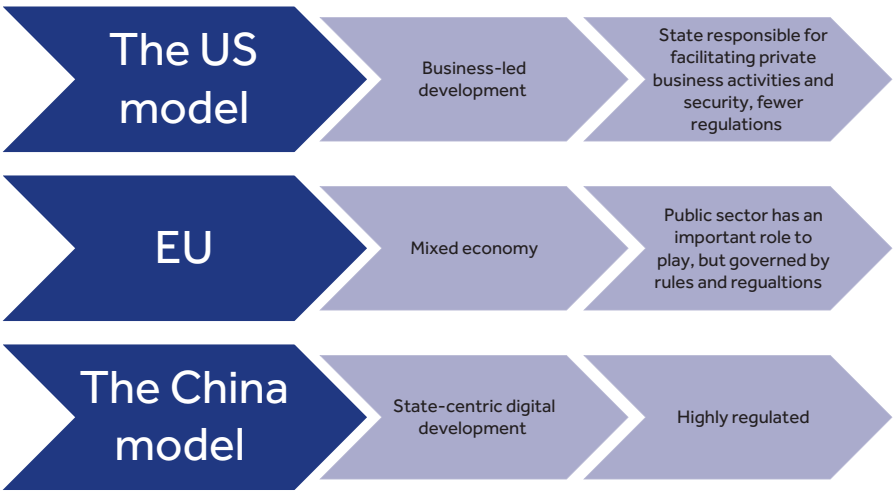
Singh (2018) suggests the issue of data protection and data flows can be examined under three distinct models, summarised in Figure 5.1. On the one end, there is the US model propagating free flow of data, driven primarily by businesses, while at the other extreme there is China's digital protectionist policies. China restricts data imports and has in place localisation policies that broadly require personal data, critical data related to internet infrastructure and user/business information to be stored locally on servers within China (Cory 2017). China also has sector-specific rules – for instance, in the financial sector, both local storage and local processing of data are required.

In between the US and Chinese models lies a mixed-economy approach, being adopted by the EU, where the public sector has an important role in building the necessary digital and data infrastructure, supporting efficient and open data markets, and undertaking regulation of the digital sector to prevent monopolistic, anti-trust tendencies or regulate areas of critical importance to the economy and society. Under the EU's new GDPR, there is one Data Protection Authority for the single market and a common digital security architecture. The GDPR has very stringent data protection provisions: it takes a consumer-centric approach to data protection that requires enterprises to provide more control and a range of rights to consumers. For instance, it requires data portability, which means that people can seek access to their data in portable forms, making it easier to switch between service providers and platforms. The GDPR takes a hybrid approach towards localisation: it does not restrict the flow of data to third countries but imposes conditions and extends its jurisdiction to any personal data processing, in the EU or abroad, that originates in the EU. However, it recognises only 12 countries to have adequate data protection regimes under the GDPR (Patel and Lea 2019).

For developing Commonwealth countries with localisation laws – such as India and Nigeria – attracting foreign investment will increasingly depend on domestic digital infrastructure, in the form of data centres, and a comprehensive and enforceable legal framework around issues of data flows, data privacy and protection. For other Commonwealth countries still in the process of drafting data legislation (see Table 5.3), Rwanda's pioneering National Data Revolution Policy (2017) provides important principles that can be adapted to its specific contexts (See Box 5.2).

Rwanda's example also brings forth the importance of 'open data'. The International Open Data Charter

Figure 5.1 Regulating the digital economy – three approaches



Source: Singh (2018).

Countries ranked in the Top 10

Malta, the UK, and Australia rank in the **top 10** out of **193** countries globally

ICT REGULATIONS

Several Commonwealth small states such and Tuvalu (189th), Solomon Islands (177th), Antigua and Barbuda (174th) and Saint Kitts and Nevis (168th) rank near the bottom

Table 5.3 Status of data legislation in Commonwealth countries

	Legal framework for electronic transactions/ e-signature?	Legal framework for data protection/ privacy online?	Legal framework for consumer protection when purchasing online?	Legal framework for cybercrime prevention?
Antigua and Barbuda	Yes	Draft	No	Yes
Australia	Yes	Yes	Yes	Yes
Bahamas, The	Yes	Yes	Yes	Yes
Bangladesh	Yes	No	Yes	Yes
Barbados	Yes	Draft	Yes	Yes
Belize	Yes	No	Yes	No
Botswana	Yes	No	Yes	Yes
Cameroon	Yes	No	Yes	Yes
Canada	Yes	Yes	Yes	Yes
Cyprus	Yes	Yes	Yes	Yes
Fiji	Yes	No	Yes	Yes
Gambia, The	Yes	Yes	Yes	Yes
Ghana	Yes	Yes	Yes	Yes
Grenada	Yes	Draft	No	Yes
Guyana	Draft	No	Yes	No
India	Yes	Yes	No	Yes
Jamaica	Yes	Draft	Yes	Yes
Kenya	Yes	Draft	Yes	Yes
Kiribati	No	No	No	Yes
Lesotho	Draft	Yes	No	No
Malawi	Draft	Draft	No	No
Malaysia	Yes	Yes	Yes	Yes
Malta	Yes	Yes	Yes	Yes
Mauritius	Yes	Yes	No	Yes
Mozambique	Draft	No	No	No
Namibia	Draft	Draft	No	Draft
Nauru	No	No	No	No
New Zealand	Yes	Yes	Yes	Yes
Nigeria	Draft	Draft	Draft	Yes
Pakistan	Yes	Draft	No	Draft
Papua New Guinea	Draft	No	No	No
Rwanda	Yes	Draft	Yes	Yes

(*Continued*)

Table 5.3 Status of data legislation in Commonwealth countries (*Continued*)

	Legal framework for electronic transactions/ e-signature?	Legal framework for data protection/ privacy online?	Legal framework for consumer protection when purchasing online?	Legal framework for cybercrime prevention?
Samoa	Yes	No	No	Yes
Seychelles	Yes	Yes	No	Yes
Sierra Leone	No	Yes	Yes	No
Singapore	Yes	Yes	Yes	Yes
Solomon Islands	No	No	No	No
South Africa	Yes	Draft	Yes	Yes
Sri Lanka	Yes	No	No	Yes
Tonga	Yes	No	No	Yes
Trinidad and Tobago	Yes	Yes	Yes	Yes
Tuvalu	No	No	No	No
Uganda	Yes	Draft	Yes	Yes
United Kingdom	Yes	Yes	Yes	Yes
Vanuatu	Yes	No	No	No
Zambia	Yes	Yes	Yes	Yes
Brunei Darussalam	Yes	No	Yes	Yes
Saint Kitts and Nevis	Yes	Draft	No	Yes
Saint Lucia	Yes	Yes	No	Draft
Saint Vincent and the Grenadines	Yes	Yes	No	Yes
Tanzania	Yes	Draft	Draft	Draft

Source: UNCTAD cyber-law tracker.

defines 'open data' as 'publicly available data that can be universally and readily accessed, used and redistributed free of charge. It is structured for usability and computability. Open Government Data (OGD) is a subset of open data, and comprises open data generated and released by local or regional government ministries, departments and agencies. In Commonwealth countries, OGD can lead to improvements in government efficiency, effectiveness, transparency and accountability. It can also lead to more inclusive policy making and government services, as well as having an impact on the economy. Australia serves as a good example of this – the Australian Government released its Public Data Policy Statement in December 2015, formalising its commitment to open data and data-driven innovation (Australian Government 2019). Geoscience Australia and the Australian National University, for instance, are using valuable Landsat satellite data for detailed mapping and analysis of Australia's land and water. With the Landsat images, Geoscience Australia has made maps of Australia's surface water patterns, providing unique information for flood risk assessment and ecosystem management.

The Kenya Open Data Initiative (KODI) is another example of a government portal that makes

Box 5.2 Rwanda's Data Sovereignty Policy

Rwanda's Data Revolution Policy has eight key principles:

i. data should be easily accessible and usable, with all non-sensitive data being open, discoverable, publicly consolidated and published on a central national data portal or other forums;

ii. raw data should be published with the highest possible level of granularity;

iii. data published should be accurate and complete;

iv. data will be published in machine-readable, modifiable format which can be openly licensed and reused, including for commercial aspects;

v. data users will recognise the author of the data throughout the process of sharing and reusability;

vi. development of an adequate legal, policy, infrastructure and privacy environment for offering data hosting services to other external governments or private data owners;

vii. exclusive sovereignty on national data but provision of hosting data in a cloud or collocated environment in data centres within or outside Rwanda, under agreed terms, and governed by Rwanda; and

viii. PPPs for building Rwanda's data industry.

Source: UNCTAD (2018).

government developmental, demographic, statistical and expenditure data available as open data, mostly in accordance with open data principles. KODI is managed by the ICT Authority, a government agency under the Ministry of Information, Communications and Technology (Kenya ICT Authority 2018). OGD was also a key enabler of the fight against corruption in Botswana; demonstrated to be an efficient tool in tracking mining revenues in Ghana; and responded to the public demand of greater accountability for the school system in Tanzania (Van Belle et al. 2018).

The case of Asia illustrates the emergence of a growing number of actors in the open data space. These include, for instance, the Open Knowledge non-profit in Bangladesh, Centre for Internet and Society non-profit in India and DataKind in Singapore (OpenData 2019) working on different issues and concerns related to transparency and accountability, public service delivery and innovation in a range of thematic sectors, such as education, health, environment, transport and economic development. New cross-regional partnerships have emerged, including the Sinar Project in Malaysia working with Phandeeyar in Myanmar to develop an app for monitoring legislative activities. However, unlike in developed Commonwealth countries such as Canada, countries in Asia demonstrate relatively few examples of open data initiatives that have originated at the state or local government levels. For example, only four of 29 states and seven union territories in India have an official open data portal. Similarly, the Bangladesh Open Data Strategy, approved in 2016, focused only on the release and publication of data at the national level (OpenData 2019).

5.2 Updating taxation policies in the digital age

The issue of taxation of digital services and content remains a 'work in progress' in many countries (ITU 2018a). On the one hand, taxation of the telecom/

ICT sector serves as an important stream of revenue for developing countries. However, on the other hand, it should not stall digital transformation and innovation within the sector. Taxation of digital services is particularly complex: digital services and content flow across borders, with countries encountering difficulties in determining where business profits should be taxed. As a result, digital giants such as Amazon and Google can exacerbate tax base erosion by transferring their intangible assets (e.g. data; intellectual property) across tax jurisdictions. Data show that only 11 per cent of countries globally apply digital services and content taxes (ITU 2018a).

Given this, UNCTAD (2018) calls for tighter regulation of restricted business practices; the break-up of large firms responsible for market concentration; regulating digital platforms as a public utility, with direct public provision of the digitised service; and strong monitoring and administration at the international level as options to regulate super-platforms. Taxing these firms where their activities are based, rather than where they declare their headquarters, can help in redistributing their rents and increase government revenues, i.e. taxing where value is created (OECD 2019). Currently, the G7 countries are in the process of discussing how taxation and fiscal policies can be revised to ensure that the benefits of the digital economy are not monopolised by the few. The G7 has agreed on a two-pronged solution to be adopted by 2020 – confirming the principle of companies being able to accrue revenues outside their legal base but also with minimum taxation, to be agreed internationally, of their activities (Rossignol 2019). For developing Commonwealth member states, requirements on data localisation may be one solution to ensure enterprises with real interests, but only virtual presence, in each country can be made to pay taxes that reflect the revenues from the economic activities they undertake within these countries (Mayer 2018).

More direct approaches have been adopted by some Commonwealth countries. For instance, in South Africa, a review of taxation in the digital economy by the Davis Committee concluded that the South African tax law provided an opportunity for foreign e-commerce suppliers to avoid taxation (Davis Tax Committee 2014). In response to the recommendations made by the Davis Committee, South Africa amended its VAT Act in 2014 to better capture the digital economy and foreign and local digital suppliers. The amendments require foreign suppliers of e-commerce services such as music, electronic books, internet games, electronic betting and software, among others, to register as VAT vendors and account for output tax provided their turnover in South Africa meets the threshold of 50,000 rand (ibid).

Australia provides another interesting case to learn from within the Commonwealth. In 2017, the Australian government passed new legislation on goods and services tax (GST) to ensure that both Australian goods and foreign low-value products were subject to the same tax regime (Australian Taxation Office 2019). There are two main kinds of taxes: a) GST on low-value imported goods, which applies to imported goods worth less than 1,000 Australian dollars ($), sold by Australian retailers or overseas retailers; and b) GST on digital products and services, which applies to digital goods and services such as music bought online or digital streaming services (ibid). Under the former type of GST, non-Australian e-commerce platforms are affected. For instance, Alibaba and Amazon may have to adjust prices for consumers in order to take into account this new tax. The latter type of GST applies to imports of digital products and services and affects merchants who sell imported services or digital products to Australian consumers and to the operation of online marketplaces. Examples of other approaches to digital taxation taken by Commonwealth countries are provided in Box 5.3.

5.3 Fostering competition in the age of digital platforms

Globally, Commonwealth countries are also facing important regulatory challenges with the rising monopolistic nature of giant e-commerce

Box 5.3 Approaches to taxation in the digital economy

1. **Singapore**: From 1 January 2020, foreign-supplied digital services will be subject to Singapore's GST. The Singapore government has already confirmed that it will likely levy 7 per cent VAT on goods and electronic services provided to consumers by non-resident companies. (Source: Quaderno.io)
2. **UK**: In October 2018, it was declared that the UK would impose a digital services tax of 2 per cent of global revenues of 500 million pounds sterling (£) from April 2020. The first £25 million of UK revenues is not taxable. The UK is currently working with the G20 and the OECD to consider how best to tax digital companies.
3. **Lesotho**: Starting from April 2018, Lesotho's Ministry of Finance decided to equate communication services VAT to that of general goods and services, which is now 15 per cent. However, this increase was staggered and not applied all at once. As such, from April 2018 communication services VAT was increased from 5 per cent to 9 per cent. Other increases will be implemented in subsequent years. (Source: ITU Tariff Policies Survey 2018)
4. **Uganda**: In 2018, the Ugandan government introduced an excise duty on over-the-top services, which is charged at a rate of 200 Uganda shillings (USh) per user per day of access. Users of any communications apps, not provided by their mobile operator, will have to pay a tax of USh200 (US$0.05) per day.
5. **Kenya**: Under the Finance Act 2018, Kenya's Excise Duty tax applicable on voice, SMS and data services was hiked from 10 per cent to 15 per cent, in addition to the existing VAT of 16 per cent applicable to mobile services.

Source: ITU (2018b).

platforms, such as Amazon and Alibaba. There are some distinct features which make it easier for a more digitalised firm to become competitive over its non-digital counterparts. Pierre and Romain (2017) highlight three such pathways. First, information and e-commerce platforms enable more efficient connection between products offered and demand, which increases transparency, facilitates information flows and results in higher consumption of goods and services. Second, the digital economy lowers barriers to entry, addresses issues of traditional non-tariff barriers and facilitates expansion in the market, increasing market contestability of digitalised firms. Third, digitalisation reinforces network effects between user groups located and interacting at different levels of the value chain.

The standard anti-competitive policies followed by many Commonwealth countries are therefore no longer able to maintain fair competition, requiring fiscal and competition policies in the digital age to be re-examined. Moreover, as digitalisation increases, investment in infrastructure that supports e-commerce will be required to successfully connect and integrate Commonwealth countries through value chains, particularly in the case of small states.

Consider the case of digital giants, which are leveraging the power of Big Data and emerging as critical intermediaries integrating across business lines and slowly taking over essential infrastructure upon which competitors depend. The extent of economic re-organisation triggered by

digital platforms is evident from how they extend themselves not just horizontally, as a connecting platform or marketplace, but also vertically (Singh 2018). For instance, Amazon is increasingly controlling the infrastructure of online commerce through its massive Amazon Marketplace, which it uses as a laboratory to sell and test sales of new goods. The Marketplace allows independent merchants to use its site to both sell goods as a retailer and host sales by other retailers, and in the process gathers massive amounts of data on other merchants, giving it a tremendous competitive advantage (Khan 2016). Furthermore, it not only charges a hefty commission fee (which goes up to 40 per cent on some products such as electronics) but also pushes its own products 75 per cent of the time, decreasing the 'visibility' of products supplied by developing country firms listed on these platforms (*The Guardian* 2016).

Contrary to many developed countries in both the earlier and current phases of digitalisation, most developing countries lack policies governing the collection and use of data (as discussed in Section 5.1), increasing the risk of their data being controlled by whoever gathers, stores and has exclusive rights on the data. The resulting increases in market concentration of digital giants and e-commerce monopolies will further focus financial power in the hands of a few leading firms in developed countries and cause increased rent seeking, anti-competitive practices and attempts to block actual or potential competitors. As a result, certain established competition and antitrust policies may no longer be adequate to address the threat posed by e-commerce giants to market competition. These policies are based on the short-term interests of consumers, and view low consumer pricing as indicative of the existence of competition. However, competition can no longer be measured primarily through pricing and output since this runs the risk of ignoring the adverse effects of 'predatory pricing' and the prospect that integration across business lines can be anti-competitive.

It is crucial that competition laws in the Commonwealth address the standard competition issues of anti-competitive agreements, cartels, abuse of dominance, and merger control, but also extend to competition challenges within the context of an increasingly digitalised economy. It is important to:

a. build capacity within competition authorities in Commonwealth countries to deal with the rising power of digital platforms and the changing landscape of competition; distinguish predatory practices from innovation-driven price reductions; and understand the power of network effects on competitiveness;

b. revise and update competition laws based on new definitions of 'market shares', which go beyond asset control to capture intangible assets such as reputation and digital control; and

c. define the relevant market in the context of digital apps and platforms that are increasingly penetrating across industries – for instance, classification of Uber as a taxi provider or technology service will facilitate the process of regulating it (ibid).

Moreover, it has become important for competition authorities to take data into account in their work – whether in terms of reviewing mergers of firm datasets that could generate durable market power, or in preventing abuse of data by dominant firms to exclude their competitors from the market (OECD 2019).

In addition to policies managing the effects of international e-commerce platforms, policies that support domestic e-commerce players are also important for African economies, which are at relatively nascent stages in terms of digitisation.[1] Therefore, more focus needs to be diverted towards enabling firms and suppliers in African countries to link up with domestic, regional and international platforms. Collaboration within the Commonwealth can help. For instance, a study by Mendez-Parra et al. (2019) on Nigeria–UK trade and investment relations highlights e-commerce as a major opportunity to overcome many of the trade barriers between the two economies in terms of both goods

Box 5.4 Jumia – opportunities and challenges to e-commerce in Nigeria

The current level of e-commerce spending in Nigeria is estimated at US$12 billion, and is projected to reach US$75 billion in revenues per annum by 2025 (Export.gov 2019). Jumia is one of the largest e-commerce platforms in Nigeria, operating in 14 African countries. In April 2019, it was listed on the New York Stock Exchange (NYSE) at a valuation of US$1.1 billion. Regionally, the largest countries for Jumia's business are Nigeria and Egypt, with overall 4 million active users at the end of 2017. The rise and success of Jumia has been complemented by government efforts in building a digitally enabling environment in Nigeria. Nigeria's economy is gradually becoming cashless, as digital payment and electronic banking are implemented in phases across most states of the federation. The adoption of electronic transactions is continuously increasing, with ATM transactions dominating the volume of electronic transactions and the Nigerian Inter-Bank Settlement System Instant Payment dominating in terms of value. This has led to increased foreign investment from Europe and Asia in Nigerian electronic infrastructure projects. Online commerce and financial technology in Nigeria is further strengthened by fast growing youth populations, expanding consumer power and increased smartphone penetration. Most customers are mobile users, which comprised 81 per cent of all traffic in 2018. To expand its supplier base, Jumia regards 'a data-driven score' as a key indicator of seller performance. It supports third-party financial services for its sellers, using this score as a way to demonstrate creditworthiness.

The government is also building a legal and regulatory framework to support e-commerce development in Nigeria. In 2015, the Federal Government signed the cybercrime bill into law to prohibit and prevent fraud in electronic commerce. The purpose of the Cybercrimes Act of 2015 extends beyond prohibiting, preventing and criminalising online fraud, but also prescribes punishments and sets the institutional framework for enforcement. The goal is to protect e-business transactions, company copyrights, domain names and other electronic signatures in relation to electronic transactions in Nigeria. In 2019, Nigeria's National Information Technology Development Agency issued the Nigeria Data Protection Regulation 2019 (the 'Regulation'), adopting several concepts from the EU's GDPR. Key elements include: a) personal data processing principles; b) requirement of consent from users for collection of data; c) that organisations must issue an easily understandable privacy policy that contains specified content; d) data security measures for protection of personal data; e) third-party contracts; f) data subject rights such as access to their personal data, getting their data corrected and restricting processing of personal data; and f) data transfers.

However, Jumia is a loss-making firm; 90 per cent of sales are from third-party sellers, and it also faces high operating costs related to warehousing, delivery, sales and advertising. Moreover, cash payments on deliveries still continue to be the dominant model of payment in Nigeria, perhaps

(*Continued*)

due to low digital trust, contributing to failed deliveries, excessive returns and late collection (ICT4D 2019). Rules on cross-border data flows also form a key issue. On the one hand, Nigeria is one of the few African countries which is a signatory to WTO e-commerce negotiations calling for harmonising e-commerce rules globally in order to support cross-border digital trade by firms such as Jumia. On the other hand, Nigeria has signed the African Continental Free Trade Agreement, in which discussions on e-commerce are at a nascent stage. The majority of African governments are keen to ensure that they are able to operate their economies appropriately, including collecting taxes and nurturing local firms, in the face of e-commerce imports.

Sources: ICTs for Development (ICT4D) 2019; City Press 2019.

and services trade. In the UK, eBay and Amazon Market Place constitute the main internet-based B2C platforms. In turn, Jumia, developed in Nigeria, constitutes the main platform to commercialise products through the internet in Nigeria (see Box 5.4 for a more detailed case study on Jumia). However, currently there is limited trade between the UK and Nigeria commercialised through e-commerce; the bilateral trade through e-commerce is generally limited to products imported through traditional channels that are commercialised through internet platforms in the respective countries. Products are sent from warehouses and other storage facilities located in the respective countries, with very little genuine direct imports from consumers. Despite the presence of a sizable British Nigerian community in the UK, Jumia has not opened a UK version of its website to allow UK-based customers to buy directly from Nigerian companies. It is important not to underestimate the role of Nigeria as a foreign investor – Nigerian firms and conglomerates like Dangote are increasingly becoming major regional and continental investors, even in the area of e-commerce.

5.4 Intellectual Property Rights in the age of digital platforms

Moreover, Commonwealth governments should consider whether current IPR frameworks strike the right balance between incentivising innovation and promoting competition. On the one hand, governments may be incentivising innovation by granting IPRs for a temporary exclusive use (i.e., a temporary monopoly), but on the other hand IPRs may be slowing the pace of technological diffusion, contributing to the decline in global convergence in labour productivity, as noted in Banga and te Velde (2018) for the manufacturing sector. Mayer (2018) argues that in the digital age, the distribution of value-added between developed and developing countries is less likely to be an issue of differences in wage rates than one of the high profit rates of mainly Northern firms that reflect rents arising from intellectual property and/or barriers to entry.

To facilitate industrialisation and reverse engineering of digitalised manufacturing in the Commonwealth, policies on data, technology transfer, source-code sharing and intellectual property will emerge as key issues. It was noted in Chapter 4 that among Commonwealth countries, Singapore has the highest ICT patent penetration, with 60 ICT-related patent applications filed under the PCT per one million people, followed by Canada, the UK, Australia and New Zealand. Meanwhile, 10 out of 33 Commonwealth small states had less than one ICT patent application per one million people in 2016, and while the other 13 countries reported zero patent penetration (World Bank data). This mirrors broader trends globally: just 10 economies account for 90 per cent of global patents and contribute 70 per cent of the world's exports of advanced digital production technologies (UNIDO 2019).

Some developing Commonwealth economies, such as India, have witnessed growth driven, in part, by reverse engineering in areas that were less patent-protected (Dahlman 2007). India successfully established a local generic pharmaceutical industry in the absence of foreign patent protection. Important lessons can also be learnt from China's growth in the digital economy – it has placed requirements for technology transfer on international firms in exchange for market access, including in some cases the transfer of source-code as a condition to sell to the Chinese government or to gain relevant licenses to trade in the country. A number of foreign companies are now engaging with Chinese companies in terms of technology transfer. For instance, IBM has shared certain intellectual property and parts of source code with China, while Microsoft has opened a subsidiary in China called Microsoft Open Tech Shanghai which participates in existing open-source and open-standard efforts. For small states in the Commonwealth which do not have enough market power to negotiate, regional strategies can be more useful, but this requires harmonised policies on data protection, privacy and stronger enforcement of IP laws to be effective.

Particularly for Commonwealth African countries and small states, intellectual property forms a key issue. However, Commonwealth countries have different levels of obligations in intellectual property treaties beyond the WTO, including participation in multilateral intellectual property treaties and commitments arising from bilateral trade agreements. Given that digitalisation may bring about entirely new products, as well as enable new functionalities and ways of use, it would appear that existing IPR protection leaves scope for active design-oriented innovation policy in developing countries (Mayer 2018).

References

Australian Government (2019), 'Open Data', available at: https://www.pmc.gov.au/public-data/open-data.

Australian Taxation Office (2019), 'GST on imported services and digital products', available at: https://www.ato.gov.au/Business/International-tax-for-business/GST-on-imported-services-and-digital-products/.

Azmeh, S, C Foster and J Echavarri (2019), 'The International Trade Regime and the Quest for Free Digital Trade', *International Studies Review*, viz033, https://doi.org/10.1093/isr/viz033.

Banga, K and DW te Velde (2018), *Digitalisation and the Future of Manufacturing in Africa*, Supporting Economic Transformation, Overseas Development Institute (ODI), available at: https://set.odi.org/wp-content/uploads/2018/03/SET_Digitalisation-and-future-of-African-manufacturing_Final.pdf.

Bauer, M, H Lee-Makiyama, E Van der Marel and B Verschelde (2014), 'The costs of data localisation: Friendly fire on economic recovery', ECIPE Occasional Paper No. 3/2014.

CIGI-Ipsos (2017), 'Global Survey on Internet Security and Trust', Centre for International Governance Innovation, available at: https://www.cigionline.org/internet-survey-2017.

Cory, N (2017), 'Cross-border data flows: Where are the barriers, and what do they cost?', *Information Technology and Innovation Foundation, May* 2017.

Dahlman, C (2007), 'Technology, globalization, and international competitiveness: Challenges for developing countries', *Industrial development for the 21st century: Sustainable development perspectives*, 29–83.

Davis Tax Committee (2014), 'Second Interim Report On Base Erosion And Profit Shifting (Beps) In South Africa', available at: https://www.taxcom.org.za/docs/New_Folder3/3%20BEPS%20Final%20Report%20-%20Action%201.pdf.

Export.gov (2019), 'Nigeria-e-commerce', available at: https://www.export.gov/article?id=Nigeria-E-Commerce.

The Guardian (2016), 'Amazon pushes customers towards pricier products, report claims', available at: https://www.theguardian.com/technology/2016/

sep/21/amazon-makes-customers-pay-more-for-popular-products-study-claims.

ICT4D (2019), 'What can we learn about e-commerce in Africa from Jumia's IPO filing?', available at: https://ict4dblog.wordpress.com/2019/04/30/what-can-we-learn-about-e-commerce-in-africa-from-jumias-ipo-filing/.

ITU (International Telecommunications Union) (2018a), *Global ICT Regulatory Outlook 2018* ITU, Geneva, available at: https://www.itu.int/en/ITU-D/Regulatory-Market/Documents/Publications/Document-Summary_English.pdf.

ITU (2018b), 'ICT Regulatory Tracker', available at: https://www.itu.int/net4/itu-d/irt/#/tracker-by-country/regulatory-tracker/2018.

Kenya ICT Authority (2018), 'Kenya Open Data', available at: http://icta.go.ke/open-data/ (accessed 14 July 2018).

Khan, LM (2016), 'Amazon's antitrust paradox', *The Yale Law Journal*, Vol. 126, No. 3, 710–805.

Mayer, J (2018), 'Digitalization and industrialization: friends or foes?', UNCTAD Research Paper No. 25, available at: https://unctad.org/en/PublicationsLibrary/ser-rp-2018d7_en.pdf.

Meltzer, JP (2015), 'The Internet, Cross-Border Data Flows and International Trade', *Asia & the Pacific Policy Studies*, Vol. 2 No. 1, 90–102.

Mendez-Parra, M, N Balchin, L Calabrese and K Onyeka (2019), 'Nigeria and UK bilateral trade and investment', ODI Report, August 2019, available at: https://www.pdfnigeria.org/wp-content/uploads/2019/08/190805ODI-UK-Nigeria-Report-058-EDF-MM-vs-0.0.pdf.

OECD (Organisation for Economic Co-operation and Development) (2019), 'Addressing the Tax Challenges of the Digitalisation of the Economy', OECD/G20 Base Erosion and Profit Shifting Project, available at: https://www.oecd.org/tax/beps/public-consultation-document-addressing-the-tax-challenges-of-the-digitalisation-of-the-economy.pdf.

Ogletree Deakins (2019), 'Kenya Introduces Data Protection Bill, 2018', available at https://ogletree.com/international-employment-update/articles/june-2019/kenya/2019-05-17/kenya-introduces-data-protection-bill-2018/.

Okal, J (2017), 'Kenya ICT Law 2016: Year in Review', available at: https://techweez.com/2017/01/06/kenya-ict-law-2016-year-review/.

OpenData (2019), 'State of Open Data', available at: https://www.stateofopendata.od4d.net/.

Patel, O and N Lea (2019), 'EU-UK Data Flows, Brexit and No-Deal: Adequacy or Disarray?', UCL European Institute, available at: https://www.ucl.ac.uk/european-institute/sites/european-institute/files/eu-uk_data_flows_brexit_and_no-deal.pdf.

Pierre, H and V Romain (2017), 'Competition Law in the Digital Economy: A French Perspective', *Italian Antitrust Review*, Vol. 4 No. 2 (2017), 85–98.

Rossignol, P (2019), 'G7 Finance Ministers and Central Bank Governors Meet in Chantilly, France', available at: https://www.france24.com/en/20190718-g7-ministers-corporate-digital-tax-gafa-deal-digital-giants.

US Department of State (2019), 'Rwanda Investment Climate 2019', Investment Climate Surveys, available at: https://www.state.gov/investment-climate-statements/.

Singh, PJ (2018), 'Digital industrialisation in developing countries: a review of the business and policy landscape', The Commonwealth Secretariat, London, available at: https://itforchange.net/sites/default/files/1468/Digital-industrialisation-May-2018.pdf.

UNCTAD (2019), *UNCTAD Rapid eTrade Readiness Assessments of Least Developed Countries: Policy Impact and Way Forward*, UNCTAD, Geneva, available at: https://unctad.org/en/PublicationsLibrary/dtlstict2019d7_en.pdf.

UNCTAD (2018), *Trade and Development Report 2018: Power, Platforms and The Free Trade Delusion*,

UNCTAD, Geneva, available at: https://unctad.org/en/PublicationsLibrary/tdr2018_en.pdf.

UNIDO (United Nations Industrial Development Organisation) (2019), *Industrial Development Report 2020: Industrializing in the digital age*, Overview, Vienna.

Waema, TM and MN N'dungu (2012), 'Evidence for ICT Policy Action – What is happening in ICT in Kenya?', Research ICT Africa, January 2012.

Van Bell, J-P, D Lämmerhirt, C Iglesias, P Mungai, H Nuhu, M Hlabano, T Nesh-Nash and S Chaudhary (2019), *Africa Data Revolution Report 2018: Status and Emerging Impact of Open Data in Africa*, United Nations Development Programme, UNECA, World Wide Web Foundation and Open Data for Development Network, available at: https://webfoundation.org/docs/2019/03/Africa-data-revolution-report.pdf.

End Note

1 However, it is increasingly difficult to understand what it means to be 'domestic' in the case of digital platforms. For instance, Jumia, which is usually seen to be "African", is owned by foreign entities, including American banks, French insurance companies and German tech firms (according to its SEC filing) and, in Jumia Kenya, around 80 per cent of the listed products are Chinese. Similarly, Alibaba is 30 per cent "African", in that South Africa's Naspers owns about 30 per cent equity.