Digital diplomacy

Technology governance for developing countries

Pathways for Prosperity Commission
Technology & Inclusive Development

Blavatnik School of Government
University of Oxford

This is a paper from:
Pathways for Prosperity Commission. (2019).
Digital diplomacy: technology governance for developing countries. Oxford, UK: Pathways for Prosperity Commission.

Cover Image: a lit-up South Africa at night can be seen on a satellite image of Earth.
Photograph: Rakchai Duangdee.
Elements of this image furnished by NASA.

Report design by Soapbox | www.soapbox.co.uk

Acknowledgements

The Pathways for Prosperity Commission would like to extend their gratitude and acknowledge the people who made this paper possible. *Digital diplomacy: technology governance for developing countries* was drafted by a team led by the Commission's academic directors, Professor Stefan Dercon and Professor Benno Ndulu, the secretariat's head of research and policy, Toby Phillips, and senior research and policy officer Beatriz Kira. Invaluable contributions to this report were made by the Commission's executive director Elizabeth Stuart, as well as Francesca Walker, Andrea Tartakowsky Pezoa, Jonathan Dolan, Putu Natih, Madeleine Chang, Bilal Majeed, and Lucinda Cadzow.

Communications and production of this paper were led by Meena Bhandari, the Commission's head of communications and events, with Philippa King, Marina Barker, Liliana Resende, and Emily Cracknell.

The team greatly benefitted from the advice of the Pathways for Prosperity commissioners, as well as Ngaire Woods, Dean of the Blavatnik School of Government, University of Oxford, together with the School's faculty and staff.

For their helpful and stimulating conversations, the team would particularly like to thank John Norris, Christopher Eleftheriades, Tunde Fafunwa, Chris Locke, Priya Vora, Kay McGowan, Michael Pisa, Emily Jones, Michael Deveraux, Sadie Creese, Juan David Gutiérrez, Kevin O'Neill, Jean-Philbert Nsengimana, Pramod Varma, Stephanie Segal, David Eaves, Kate Wilson, Ify Ogo, Martin Kohout, and Mactar Seck.

The depth of the report is thanks, in part, to: independent research and analysis conducted for the Commission by Future State; respondents to the Commission's survey; interviewees who participated in consultations; participants of the roundtable discussions in Washington DC, Bali, Kigali, and Oxford; and background paper authors, Parminder Jeet Singh, Joanna Świątkowska, Mariana Giorgetti Valente, Vikas Gupta, Kay McGowan, Priya Vora, Matthew Homer, Jonathan Dolan, and Prakhar Misra.

About the Pathways Commission

The Pathways for Prosperity Commission on Technology and Inclusive Development is proud to work with a diverse group of commissioners who are global leaders from government, the private sector, and academia.

The Commission is based at Oxford University's Blavatnik School of Government. We collaborate with international development partners, developing country governments, private sector leaders, entrepreneurs, and civil society to produce cutting-edge research.

The Commission aims to catalyse new conversations and to encourage the co-design of country-level solutions aimed at making frontier technologies work for the benefit of the world's poorest and most marginalised men and women.

Contents

Executive summary

Current approaches to governing, managing, and regulating digital technology, such as they exist, are dominated by a small number of countries, and based on the priorities of developed nations. The business models and digital architectures designed by firms can have far-reaching impacts, and these are inherently shaped by the regulatory environment. Despite this, surprisingly little attention is paid to how poorer or resource-constrained countries should approach digital regulation – either within their own countries or as an increasingly pressing transnational issue.

The Pathways for Prosperity Commission undertook a consultation with policymakers in developing countries to identify their key technology policy priorities, specifically in terms of international coordination.[1] Emerging governance mechanisms around the digital economy will be pivotal for those seeking to make the most of the opportunities on offer. However, to date, developing countries' priorities have not been heard. Specifically, the consultation sought to identify what rules and policies to govern cross-border provision of digital services would help to ensure that all countries share in the gains of the data-driven global economy.

For developing countries, governance and regulation for the new economy is a daunting task, but concerted international cooperation can help. As our analysis of the consultation reveals, international coordination presents an opportunity for developing countries to exercise their own voices and develop a governance model that works for them. Countries can work together to resolve many of the issues listed below.

What are the key technology policy priorities for developing countries?

The results of our consultation

- **Developing countries should be able to tax technology companies that offer goods and services to their residents.** Governments in developing countries have little ability to tax businesses that participate in the economic life of their country without an associated or meaningful physical presence. International cooperation can help to ensure that developing countries get their fair share of the revenue generated by foreign technology companies.

- **Developing countries need support from the international community to combat cybercrime and improve cybersecurity.** Developing countries are particularly exposed to cybercrime, which causes financial and reputational losses. International cooperation that involves developing countries can improve cybersecurity to enhance trust amongst actors and foster investment in developing countries.

- **Frameworks to protect privacy and personal data should conform with developing countries' policy priorities.** Developing countries need to establish rules to ensure that citizens have control over their personal information, and to prevent unauthorised or arbitrary use of their data by private and public agents. International cooperation can help with peer-learning and technical standardisation, but individual countries should decide for themselves on the best data governance framework that works for them.

- **The design and enforcement of competition laws need to be fit for the digital age.** Digital technologies are straining existing best practice approaches to competition policy, and this challenge is particularly daunting for developing countries, many of whom are only just beginning to implement existing best practice. International cooperation can support capacity-building, information sharing, and coordinated responses.

- **Developing countries' interests must be considered in intellectual property (IP) rules.** IP rules can diminish developing countries' access to technological innovations or impose costly compliance requirements on their firms, restricting their capacity to engage in parts of the global digital value chain. Developing countries can give a voice to their interests through coordinated action between like-minded states.

- **Data often has incredible potential beyond the initial purpose for which it was collected, but the tools, standards and regulations that would enable data sharing are largely absent.** Transactions that can lead to inclusive growth are increasingly dependent on data being transferred across the world. As data can be used multiple times without losing its value, interoperability opens up the possibility for new and innovative uses, increasing economic efficiency. International cooperation can help establish shared standards to make services and applications work seamlessly with each other.

The six policy priorities outlined in the box above span a broad range of technical and ideological issues. Countries will need to determine their policy settings and resolve trade-offs based on their domestic values and preferences. Indeed, many of these problems are ones of domestic policy – and yet, because of the inherently globalised nature of digital products and services, international coordination can play a key role. Five principles emerged repeatedly during our consultations. They can help guide efforts to make the cross-border governance of digital technologies work for developing countries.

How to make cross-border governance of technology work for developing countries

Key principles for a cooperative digital world

Foster digital cooperation: creating incentives for countries to work together. Large global institutions are unlikely to solve the problems of digitalisation for developing countries. Developing countries should chart their own path towards international cooperation to shape cross-border regulation of technology. This could start with regional coalitions or agreements between non-regional groups of countries with shared values and goals. It may also be easier to start with less contentious topics, such as online harms, and then evolve to address wider issues, such as taxation.

Tailor technology governance for developing countries: better ensuring implementation in a wider range of national contexts. Global rules and standards are often not a good fit for developing countries, which have capacity constraints and policy goals that often differ from those of developed nations. Any set of rules with impacts outside the borders of a single country should consider a tiered approach, starting with a minimum-implementable baseline that any country could (reasonably) be expected to meet in order to engage with cross-border digital trade.

Unlock data for inclusive development: using data to improve people's lives. Much of the world's information is locked away in proprietary databases, employed only for a slim fraction of its possible uses. Data governance rules should give people the ability to access their personal data and provide policymakers with tools to aggregate across anonymised datasets, maximising the social and economic value of data. This should be accompanied by adequate levels of protection to prevent arbitrary abuses of data (eg unauthorised mass surveillance).

Be part of something bigger: harmonising cross-border digital trade. The digital economy is increasingly dependent on data being transferred across locations, systems and devices. Digital integration can generate immense value for countries and supercharge innovation. Countries could work together to support cross-border digital trade that is as frictionless as possible. This will require some level of shared standards and interoperable systems – ensuring that digital goods meet consistent requirements and standards.

Protect against cyber harms: establish data protection, transparency and accountability measures. People, governments, and businesses need to feel safe to invest and participate in the integrated digital market. This will require a consistent regulatory framework that gives users trust and confidence in service providers, improves legal certainty, and fosters investment. Transparency and accountability mechanisms could improve the reliability of automated decisions and help to prevent algorithmic discrimination.

Successful implementation of these principles will depend on embedding them into the wider political economy, taking into account each country's unique needs and priorities.[2] Some of these principles are inherently cross-border, while others demand both domestic and international approaches: but they all describe outcomes that could be achieved through international cooperation, and that could improve people's lives in developing countries. Such principles, however, will not be pursued in a vacuum, rather their implementation will largely depend on complex negotiations at national and international levels.

Governance decisions made today will have far-reaching consequences in the emerging digital economy. New technologies bring countless opportunities, but they also bring risks, not least the risk that only a small number of powerful states shape the digital future for everyone else. But it does not have to be this way: it is possible for governance and regulatory regimes to support the interests of developing countries. International coordination between like-minded nations will be crucial in governing a digital economy that works for everyone.

Chapter 1
Introduction

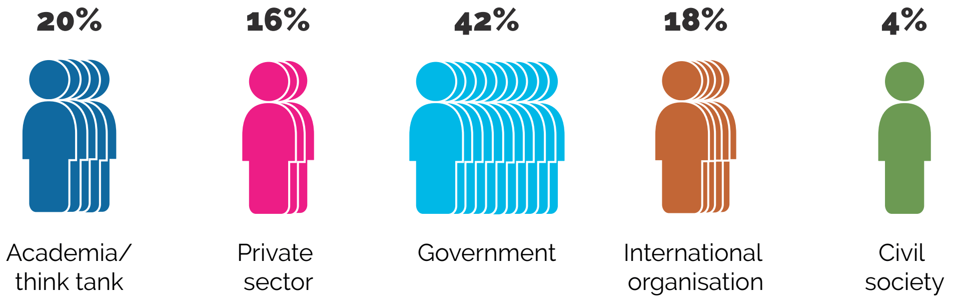
The use of digital technology is growing at an extraordinary rate. The global volume of digital information doubles every two years and is set to reach 175 zettabytes (175 trillion gigabytes) by 2025.[3] This will only increase as the next 3 billion people come online.[4] For those already online, digital products are becoming more and more integrated into everyday life, as prices of devices and applications fall and innovations multiply. The volume of global digital commerce exceeded US$3 trillion in 2017, representing 13% of total commerce, and is set to more than double by 2022.[5] Data flows now account for a larger share of GDP growth than the global trade in goods.[6] Industries that were once purely analogue, such as food delivery or maize farming, now benefit from digital integration. This transformation continues apace, rapidly creating new and unforeseen opportunities and disruptions.[7]

The current wave of technological change is largely driven by data – many new products are based on the ability to store, move, and analyse pieces of information. The movement of data is practically frictionless: it can be transported across borders and stored or processed anywhere in the world at almost no marginal cost. The practical reality of this is that the booming digital industry is globalised by default. A successful digital product can easily move into new markets, and the availability of microservices makes it much easier to provide digital services in this global market.[8] For example, when a passenger calls a car using Indonesia's Go-Jek's ride-hailing app, their information first goes to a cloud computation service (owned by Google and based in Singapore), from which point the app can locate an available driver and calculate the price of the journey.[9] The driver will receive the information about the ride on their phone and use Google Maps to navigate the traffic, sharing real-time location data with the cloud service.[10]

But while technological change is dynamic and fast-paced, many laws and policies for regulating and governing technology remain static. Regulatory tools that were developed decades ago are being applied to unrecognisable problems in the digital age. The lag in regulatory best practice and technical assistance means that this issue is all the more prevalent in developing countries, which do not have the appropriate rules or means to enforce them adequately. For example, many developing countries are struggling to design and implement a competition policy regime fit to deal with digital platforms, the likes of which are already under strain in richer nations.[11] Malawi, for instance, only created a competition authority in 2012, and Malaysia only in 2010. Benin and Mongolia are amongst the countries that are yet to establish one.

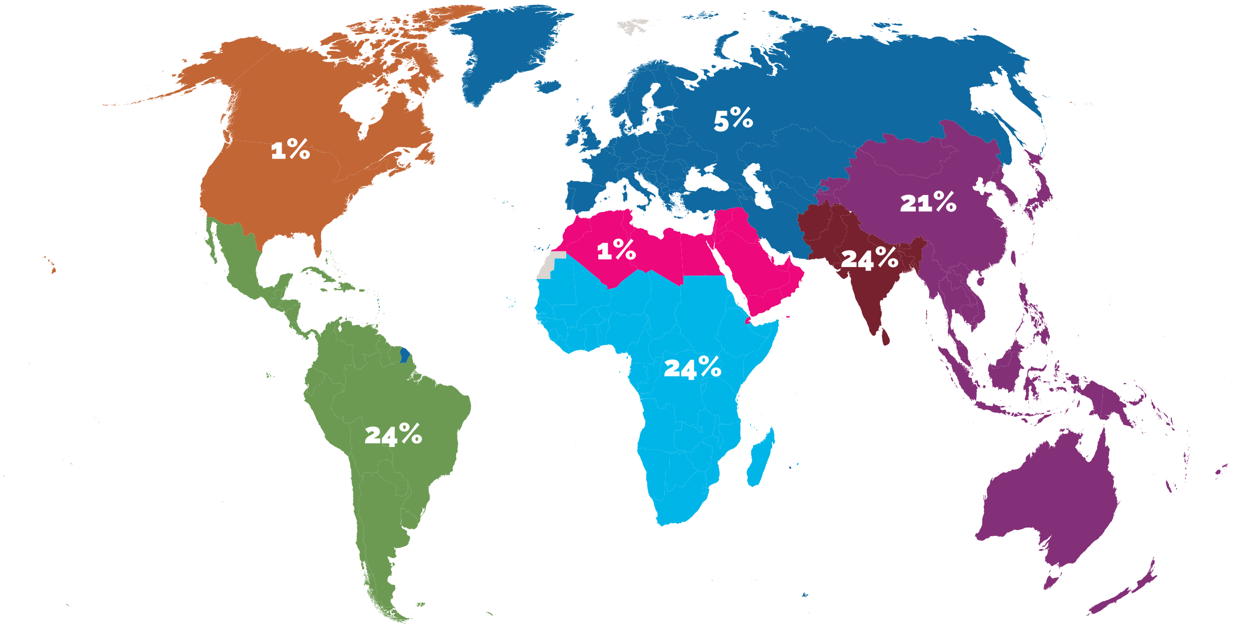
The Pathways Commission undertook a consultation to identify the technology policy priorities that will make a difference in improving the lives of people in low- and middle-income countries. We consulted more than 100 stakeholders to develop a more nuanced understanding of the key challenges and opportunities of the digital age from the perspective of developing countries. A total of 105 people completed a survey and 12 participated in interviews with open-ended questions (see Figure 1). 91% of survey respondents were from developing countries (see Figure 2).[12] Detailed findings, and a discussion of the methodology, are presented in a forthcoming paper, but in Chapter 2, we present the highest-ranked policy issues requiring coordinated international action.[13]

Figure 1. **Distribution of survey participants based on stakeholder group**



Note: This figure does not include two respondents who identified their stakeholder group as 'Other'.

Figure 2. **Distribution of survey respondents based on the region of primary expertise**



Note: This figure does not include 19 respondents who identified their region of expertise as 'Global'.

Despite the fact that many of the policy levers in the digital age sit within reach of domestic policymakers, there are challenges that will require international coordination. This was a common concern among consultation respondents. Countries can, in theory, act unilaterally to resolve many of the identified policy issues. Initiating change in many of these issue areas – from privacy to competition policy – is within the remit of domestic policymaking, and requires each country's government to balance digital change with other national priorities. However, as we further explore in Chapter 3, there are benefits from coordinated action, both at the regional and international levels. In reality, the lack of international consensus limits countries' available options to act unilaterally – they often lack the political heft, technical capacities, and voice to influence major technology policy debates. Even when individual countries do act independently, their limited options can result in blunt decisions that prove ineffective or that enhance inequalities.[14]

Many of the pressing concerns of the digital age can only be effectively tackled by cross-border regulation and data-sharing mechanisms between countries. Without such cooperation, the consequences for individual countries, their businesses, and their citizens, may be significant. For example, a survey participant from Indonesia expressed concern with the prospects of their country achieving its policy goals on its own:

> **'the country is still figuring out how to support, incubate, and accelerate technology for its own good, let alone setting up a robust technology policy independent of global examples to take inspiration from'.**
> Survey respondent

Even though debates about the challenges of digitalisation are starting to take place at international organisations such as the World Trade Organization (WTO) and the World Intellectual Property Organization (WIPO), solutions that work for developing countries are unlikely to emerge from current multilateral institutions, as their voices are less likely to be heard and so their priorities not reflected in the debates taking place in these fora.[15] In Chapter 4, we propose an alternative agenda to support developing countries to truly harness the potential of frontier technologies.

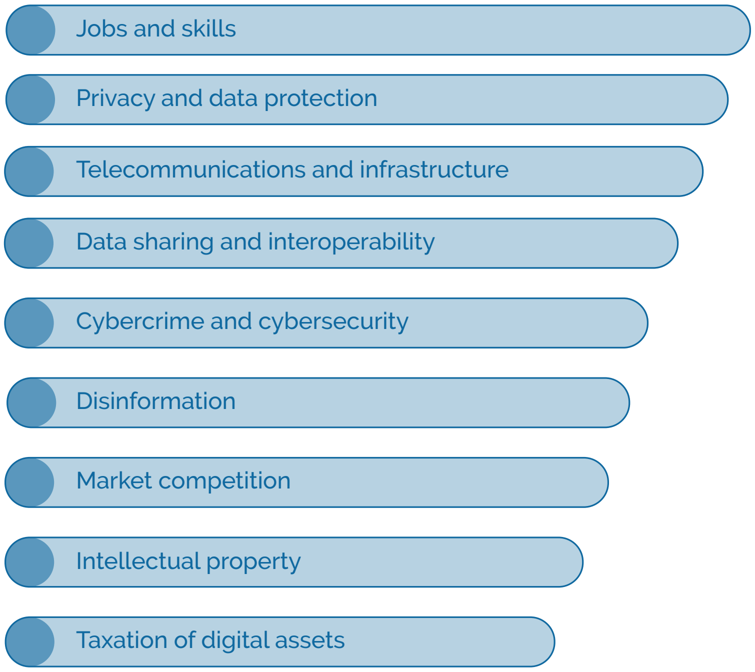
Chapter 2
Technology policy priorities for developing countries

The global debate around technology governance is firmly focused on a few centres of power: the US, the EU, China and, to a lesser extent, India.[16] These countries have the main driving roles in most policy discussions around the world – often with competing interests, as illustrated by the US-China trade war. The same holds true for governance of technology: with so many powerful – and, at times, rivalrous – perspectives on how to regulate in the digital age, the concerns of the majority of developing countries are often left out of the picture. Therefore, understanding the policy priorities that would make the most difference for developing countries was at the heart of the Pathways for Prosperity consultation process.

The Pathways consultation revealed that the most important priority for developing country policymakers is economic development. Respondents identified 'jobs and skills' – the measure most entwined with economic development – as the most significant issue by any measure (see Figure 3).[17] Any agenda for digital governance must therefore recognise, and ideally support, this imperative. The path for digital-led development, however, is not straightforward. The consultation found that, when addressing the challenges of digitalisation, policymakers try to balance economic development, national security, and citizen rights – priorities that may sometimes be in direct tension with each other.

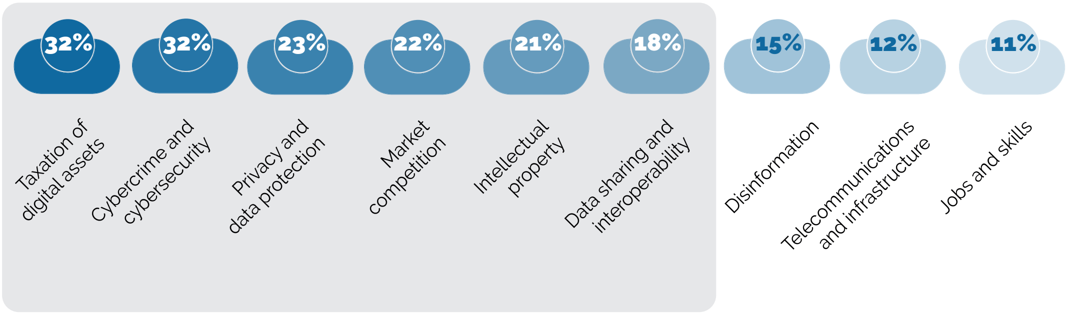
Policy issues which prevent developing countries from harnessing the opportunities of new technologies are not just questions of domestic policy: they often require concerted international cooperation. Our survey revealed six areas where global efforts are most needed (see Figure 4). In this chapter, we discuss these six areas: taxation, cybercrime and cybersecurity, privacy and data protection, market competition, intellectual property, and data sharing and interoperability. We discuss how digital technologies give rise to challenges around each of these issues, and the developing countries' perspectives on these challenges. While recognising that there are a plethora of other policy priorities which are relevant for developing countries, we believe that these other issues are either already covered by existing global frameworks and institutions, or are a matter of domestic policymaking.

Figure 3. **Respondents' ranking of policy issues**



Note: Ranks were calculated using the Rank Sum Weight Method.

Figure 4. **Percentage of respondents who identified lack of international coordination as an obstacle to achieving a policy priority**



2.1 Taxing digital assets is challenging for everyone – in particular for developing countries

The digitalisation of the global economy poses a series of challenges for taxation which require international coordination, not least because many technology companies are multinational corporations. Technology companies can be registered in one country while offering goods and services worldwide, as digital services do not require a physical, in-country presence and can be delivered from afar.[18] This allows multinational companies to book their profits (and thus pay corporate tax) in the (often richer) countries in which they are based.[19] This scenario affects both developed and developing countries and is not altogether new – indeed, it is the fundamental problem of multinational taxation in a globalised world – but it is made more difficult by the intangible, fluid nature of digital goods and the digital economy.[20]

Developing countries represent a large share of digital services' user base, but are unable to collect taxes from their profits. For example, almost 1.4 billion people in developing countries are Facebook users, representing almost 70% of active users worldwide (although they account for a smaller share of global revenue).[21] It is common to see firms for which the only parts of their business that 'exist' in a developing country are their customer base and a facility to receive payments. It is still possible to tax the *transaction* when money changes hands (several countries apply their regular goods-and-services consumption tax to digital goods), but the *profit* and the rest of the business remain abroad.[22] This is not a problem if we assume that the product is created entirely in a foreign country and merely imported whole, but that is not necessarily the case with digital services that, for instance, rely on local data. As a result of such tax arrangements, technology companies often fail to contribute a fair share to national revenues, fuelling further economic inequality, and limiting funds available for education, health, and infrastructure.

The interconnectedness of the data-driven economy and the different revenue models adopted by technology companies – in which many services are offered for 'free' – add another layer of difficulty to the taxation of digital assets. Traditional taxation, at its foundation, attributes value to a transaction – but this falls apart when obviously valuable transactions and services do not carry a price, or when it is unclear where or how the value is created. Challenges include addressing how digital services and the data that enables them should be characterised and valued for tax purposes (see Box 2 on measuring the value of digital transactions), and how to distribute this value among the actors and countries involved in the operation.[23] A particular concern is whether any profits attributable to the remote gathering of data by a company should be taxable in the country from which data is gathered.[24]

Developing countries have – understandably – been implementing measures to try to capture some of the wealth generated by digital transactions, but this has caused considerable controversy. In countries under significant budgetary pressure with low-capacity taxation systems, digital technologies can help to improve tax administration.[25] However, in most developing countries, taxing digital services has been considered a more immediate means of securing extra revenue. Other approaches have included India's equalisation levy on local businesses that procure digital services abroad, or Uganda's move to levy users through mobile network operators (who do have a taxable presence) for the use of social media or messaging (see Box 1).[26] Despite the growing criticisms of such measures, it is important to acknowledge that, in many cases, they are the only alternatives available for developing countries struggling with their finances. If corporate actors were more proactive in finding ways to contribute to the economy of the countries in which they operate, there would be fewer incentives for the use of 'sticks' – not only including social media taxes, but also measures such as data localisation and interruption of app service provisions (which are widely condemned by technology companies, civil society organisations, and users themselves).

Box 1. **How have developing countries attempted to tax digital transactions?**

Uganda's social media tax

In 2018, Uganda introduced a 'social media tax', which charged users 200 Ugandan shillings (UGX) (around US$0.05) per day for the use of a number of internet applications, including popular services such as Facebook, Twitter, WhatsApp, and Instagram.[27] The new tax adds up to about US$1.50 per month or US$19 per year, in a country where many people live on less than US$1 a day.

In the period after the introduction of the tax, data use and mobile money transactions decreased in Uganda, and internet user penetration dropped from 47% to 35%. In a series of tweets, the Uganda Communications Commission (UCC) announced that, following the imposition of the social media tax, the number of 'over-the-top' (OTT) subscriptions had declined by more than 2.5 million in the last quarter of 2018.[28]

The tax also disproportionately affected marginalised users – the cost of the social media tax represents 2.4% of average individual income in metropolitan Kampala, but 22.6% of the average individual income in rural Bukedi.[29]

India's equalisation levy

India implemented an equalisation levy on cross-border digital advertising in June 2016.[30] The 6% levy applies to payments made by companies based in India to a foreign company (without a permanent establishment in India) for online advertisements, if the annual payments exceed Rs.100,000 (approximately US $1,450) in one financial year.[31]

The levy, which is only applicable to cross-border business-to-business (B2B) transactions, is withheld at the time of payment by the purchaser of the services (ie the Indian firm hiring the advertisement services), and subsequently paid to the government. The measure is controversial because it puts an extra burden on *local firms* using foreign platforms for advertisements, and is especially heavy for startups. However, it has contributed to an increase in tax revenue: the Indian government reportedly collected approximately US$76 million between 2017 and 2018 through the equalisation levy.[32]

A government committee has been analysing measures for other types of cross-border digital transactions, but the equalisation levy has not yet been expanded to other sectors. However, the Indian government has considered other measures to tax digital transactions, such as the introduction of a 'significant economic presence' (SEP) concept, which would allow the government to tax income of foreign companies based on their *virtual* economic presence.[33]

Reforms are required in international taxation to ensure that developing countries share in the benefits of global technological progress in an inclusive way. Current tax treaties prohibit the taxation of business profits of companies without a physical establishment in a country.[34] Changes in international taxation might contribute to the ability of developing countries to tax businesses that are part of the economic life of the country, but which do not have an associated or meaningful physical presence. Ideally, countries would have a fair mechanism to tax virtual goods, which does not unduly deter domestic players from participating in digital markets. Developed countries – through fora such as the G7 and the Organisation for Economic Co-operation and Development (OECD) – are starting to respond to this problem.[35] The OECD's recommendations include adopting the concept of a non-physical taxable presence, and efforts to identify and define income derived from a particular source in a jurisdiction. Another measure could be a global tax. This would tax multinational enterprises on their global income at a minimum rate, regardless of where they are headquartered, and distribute the revenue according to the proportion of the profits generated in each country.[36]

2.2 Managing cybercrime and cybersecurity are high priorities in developing countries

While technology presents many opportunities, it also comes with new threats of cybercrimes – such as malware attacks, fraud, and abuse of data – which affect prospects for inclusive growth. Putting a number on the cost of cybercrime is challenging, but evidence shows that global losses are immense. Recent estimates from the International Monetary Fund (IMF) and a study from the Centre for Strategic and International Studies (CSIS), in partnership with the company McAfee, have estimated the annual costs of cyberattacks and cybercrime as US$350 billion and US$600 billion, respectively.[37] Cybercrime also entails important non-monetary damages to innovation, national defence, competitiveness (of both countries and companies), and prospects for economic growth.

This is a global challenge: as cyberthreats can originate anywhere around the globe, the scope of the problem is inherently international. Criminal investigations and law enforcement activities, in contrast, are usually restricted by national jurisdictions. When information is stored outside a jurisdiction, it can become difficult for law enforcement agencies to retrieve and act on the information that is relevant to their work.[38] It is also hard to trace the precise originating location of a cyberattack.[39] As an increasing proportion of economic activity relies on digital infrastructure, losses from cybercrime will only grow if there is no improvement in international cooperation.

Developing countries are particularly exposed to cybercrime and cybersecurity risks. The combination of less stringent legislation, lower digital literacy, and less robust digital infrastructure makes developing countries more vulnerable to cybercrimes.[40] Although similar challenges confront both developing and developed countries, the optimal solution for each country will differ depending on their resources and capabilities, as not all countries would be able to implement enforcement mechanisms that demand highly technical skills or state-of-the-art equipment. Specific challenges for developing countries include a lack of appropriate laws and enforcement authorities, lower levels of self-protection measures (eg due to lower digital literacy), and a lack of private sector support.[41]

In light of so many limitations, developing countries have struggled to find appropriate policy responses.[42] Some nations impose policy and regulatory restrictions on the movement of data. This can be for many different reasons, including to protect the data from attacks and to grant relevant authorities access for law enforcement purposes.[43] For example, Vietnam's cybersecurity legislation requires 'aggregated information websites' and social networks to operate at least one server in Vietnam and provide user data to the government when requested.[44] While laws requiring data to be hosted within a particular jurisdiction might in theory facilitate oversight and regulation by local authorities, there are many risks associated with these strategies.[45] These policies are likely to increase costs for digital products and could actually make data more vulnerable by forcing firms to concentrate a significant amount of their information in one place (creating a target for attacks and facilitating potential government hacking and mass surveillance).[46] Moreover, issues relating to conflicting laws may still emerge: if the physical server is located in one country, but the company holding it is headquartered in another country, it may still be subject to the latter's laws.

Governments can use a range of policy tools, and potentially come together to achieve similar objectives: pursuing international cooperation to this end may prove a beneficial strategy.[47] One approach would be to improve cross-border arrangements to share data for law enforcement purposes (as will be discussed in Chapter 4). The existing global processes are governed through general mutual legal assistance treaties (MLAT), which are slow and cumbersome when law enforcement authorities request access to electronic data.[48] The negotiation of specific *digital* information-sharing agreements for law enforcement purposes offers a promising solution; one that would give digital businesses a strong understanding of the legal environment in which they are operating (enhancing legal certainty). This would act as an incentive for investment in the digital sector, as firms will be less fearful of undue fines or lawsuits.[49] It would also provide protections against abuses by governments and other ill-intended agents.[50] The US, for example, has the CLOUD Act, which sets criteria for data to be stored on international servers, and the EU's e-evidence legislation creates a simplified framework to retrieve data between EU member states.[51] A coordinated group of developing countries could create similar frameworks, but ones that take into consideration the particular constraints of developing countries. As we discuss in Chapter 4, this could be implemented through a risk-weighted approach and a progressive framework, establishing different levels of data sharing. Further cooperation to address cybercrime could also cover harmonised criminalisation and procedural powers, for example. This would go some way to facilitate digital trade between developing countries, building bridges, rather than fostering a series of digital islands.

2.3 Frameworks to protect privacy and personal data are fundamental in a digital age

Privacy and personal data protection are central issues in the digital age, and different countries have different perspectives on how to address them. Digital technologies make it possible to collect, store, and process enormous amounts of data in a centralised way, which reduces individuals' control over their own data. As a result, the risk of exposing their private lives increases. While this challenge is universal, the extent to which privacy and personal data are protected varies according to social, political, and cultural contexts. The concept of privacy as a right itself is not uniformly adopted in all jurisdictions around the world.[52]

Developing countries are concerned with governance of personal data and implementing an appropriate framework to protect this important asset of the digital age. Only 36% of developing countries currently have data protection and privacy legislation in force.[53] However, with the growing importance of the digital economy, the number of developing countries establishing rules or frameworks around data management is on the rise.[54] This was also a top priority among the policymakers we consulted.[55]

Mounting evidence suggests that it is necessary to have some guidelines about how personal data is collected, stored and transferred.[56] People should be able to understand and have some control over how, and for what purpose, their personal data is used. The real challenge is developing a framework that protects people's privacy while eliciting the best economic and social value from personal data, for the individual and society.[57] Perhaps more challenging are cases where data is connected to an individual but is not necessarily 'personal' or 'sensitive' data (as they are usually defined). In such cases, there are questions as to whether the same privacy rules that apply to personal data should apply to other sets of data, such as drone imagery of a village.[58] Finally, data protection is important in preventing abuses inflicted by governments themselves, so relevant frameworks should acknowledge the possibility of abuse and establish provisions to hold authorities and companies accountable.

The international debate on the development of standards for privacy and data protection has been mostly driven by big technology companies and the governments of developed nations, often disregarding other social norms and expectations. Governments have been developing standards for data protection that apply beyond the borders of a single jurisdiction. The most evident example of regulation is the EU's General Data Protection Regulation (GDPR), which is becoming a de facto global benchmark, due to the extraterritoriality of its provisions, and also to growing pressure in international policy circles for more countries to adopt similar terms.[59] For example, one of the survey participants stated that:

> **'GDPR has definitely influenced India's draft data protection bill'.**
> Survey respondent

Private companies' terms and conditions and privacy policies are also often applied worldwide. These standards, however, are often disconnected from developing countries' priorities. In many cases, policymakers must balance various, and sometimes competing, interests. There are important trade-offs to consider when it comes to protecting data. While data protection rules are important to protect users and build trust (as we discuss in Chapter 4), there is a range of ways to implement them. The question of where to draw the line is one for individual countries. High standards of data protection risk raising the cost of doing business and potentially hindering innovation. Some argue that this is a good thing – internalising the risk (incorporating data protection concerns into a company's decision-making) and only preventing innovation that would put users' data at risk – but this depends entirely on the country's risk preference and how the rules are tailored.[60]

2.4 Competition laws and their enforcement need to be fit for the digital age

Competition cases involving digital markets increasingly have a cross-border dimension. Technology companies are now global and affect the everyday lives of citizens worldwide. Any action or decision taken by one country is likely to have spillover effects elsewhere. For example, after an investigation by the German competition authority into Amazon's German marketplace, amazon.de, the company agreed to change its terms of business for sellers' activities. Amazon did not just make this change in their European marketplaces; they implemented these new terms in all marketplaces worldwide, including in North America and Asia.[61]

New technologies have given rise to innovative business models which challenge competition law and enforcement. Features of digital platforms make enforcement of competition policy even more technical – for example, identifying the relevant market, understanding the role of data in creating a product, and dealing with competitive dynamics that are not manifested in prices, among other challenges.[62] Also, many of the most popular social media platforms and search engines do not charge consumers, as their revenue comes from advertisers and services in 'other sides' of the market, making traditional competition tools inapplicable. Other platforms do not offer a direct service at all, but merely take a cut from the exchanges they facilitate (for example, between a driver and a passenger). Digital technologies also offer new opportunities for practices that prevent or reduce competition in a market, such as facilitating virtual collusion – for example, when humans intentionally use algorithms as a tool to coordinate behaviour and set higher prices, or when algorithms independently collude using machine learning to 'follow' the price leader (introducing parallel behaviour).[63] Furthermore, digital markets have a stronger tendency toward concentrated structures, due to economies of scale and scope, and stronger network effects, making it easier for companies to lock in users.[64] For example, once a company has built a business analytics tool, they can deploy it to new customers at almost no additional cost.

Regulating for competitive markets can be a particularly daunting challenge for developing countries. Many developing countries are not equipped to enforce competition policy in bricks-and-mortar markets, and often lack the capacity and resources to analyse and address new issues in digital marketplaces.[65] Several Latin American countries are still drafting national competition laws.[66] In sub-Saharan Africa, almost every country has a competition law in place, but few countries have established adequate institutions to implement, monitor and enforce their competition policy.[67] Authorities in developing countries are often constrained by scarcity of resources, including a scarcity of trained experts, meaning that in some places, competition policy remains little more than words on a page. Malawi, for example, first enacted its competition law in 1998, but the competition authority was only created in 2012. In the Dominican Republic, the competition law was enacted in 2008, but the authority only started operating in 2017.[68] Meanwhile, in Mali, Niger and Benin, the enforcement authorities are not independent and do not have their own decision-making power.[69]

Developing countries also face challenges in keeping their markets open to entry and innovation. Competitive markets are key drivers of economic growth and productivity, but there may be particularly strong pressures to protect incumbents, especially during periods of structural change.[70] Such behaviour would constrain entry to a market, and incumbent power would impact on innovation and future economic growth potential. Even where startups do enter the market, they may soon face competitive pressure and may eventually be acquired by dominant platforms.[71] While this is true for both developing and developed countries, countries with low technical and political capacities and limited resources are less equipped to deal with attempts from incumbents to entrench market power.

In the face of the rapid and global digitalisation of the economy, coordination mechanisms can help policymakers to stay abreast of developments and to learn from each other.[72] The number of jurisdictions with competition law enforcement jumped from fewer than 20 in 1990 to about 120 in 2014.[73] As the number of authorities around the world continues to grow, coordination between them will be ever more important.[74] The International Competition Network (ICN) is one arena for exchange of experiences, and had more than 130 member competition authorities in 2019. The African Competition Forum (ACF) is also widely recognised as an arena for peer learning and information sharing between authorities in Africa.[75] Competition authorities have successfully cooperated in the past. For example, the acquisition of Monsanto by Bayer in 2016 was reviewed in 29 countries, and several authorities cooperated very closely to reach a decision – including the authorities in the EU, US, Australia, Brazil, Canada, China, India and South Africa.[76]

2.5 Intellectual property rule-making needs to reflect the interests of developing countries

Global policymaking around intellectual property is commonly recognised as an obstacle for developing countries' policy goals.[77] The relevance of data in the digital economy, the emergence of new platforms for sound and image reproduction, new possibilities for user-generated content, and the boom in the 'knowledge economy' based on intangible assets, all provide opportunities for widening access to information and for generating wealth.[78] While new technologies have reduced technical and cost barriers to copying and sharing intellectual property (IP), laws and policies exist to protect the rights of IP owners. Intellectual property rights are fundamental to foster technological innovation and bring valuable new products (goods and services) to market.[79] The historical evolution of such rights has always been connected to technological and scientific developments, and the new discussions on IP taking place around the world are no different.[80] However, in some cases, IP rules and broad protections, such as patents and trade secrets, can have the effect of diminishing developing countries' access to knowledge and information, and restrict their capacity to engage in certain parts of the global digital value chain.[81]

The international debates around changes in IP governance are strongly dominated by richer nations. Developed countries, where most of the world's IP-intensive and large technology companies are based, use their political heft and influence to directly push their interests in bilateral and multilateral agreements.[82] These countries, understandably, aim to protect the results of their firms' investments in research and development, not only within their borders, but also in other parts of the world. As a result, developing nations are often pressured to conform with norms around IP rights.[83] In other cases, developed countries adopt rules that have effects outside their territories, limiting options for policymakers and businesses in developing countries. The EU Copyright Directive, for example, will require online content-sharing service providers who wish to enter the EU market to use appropriate technology to prevent the uploading of copyrighted content. In practice, this requires costly filters or active moderation. Given the cost of deploying such efforts, the law may entrench the dominance of big firms with deep pockets and prevent new entrants from accessing the European market.[84]

Developing countries often lack the political heft and technical support to push forward their interests in international negotiations. Different countries push their respective agendas in international fora such as WIPO, which leads the development of IP frameworks. A significant amount of IP governance is also pursued through trade agreements. However, current negotiations within these spaces do little to help people in developing countries access information products.[85] For example, the e-commerce agreement under negotiation at the WTO proposes new rules to further protect algorithms (which already enjoy copyright protection) and could allow the emergence of new monopolies over data.[86] Trade negotiations in IP can be stacked against developing countries with take-it-or-leave-it 'package deals', secret negotiations between sub-groups, and a lack of measures to balance IP restrictions, such as licensing agreements.[87] Thus, a crucial factor in achieving more favourable outcomes for developing countries is through an increase in their bargaining power.[88] Developing countries should be able to have their voices heard in IP debates, not only to protect their IP but also to have their development interests represented. This could be accomplished, for example, through regional cooperation (as we discuss in Chapter 4), and by fostering the use of open software and open data.

2.6 Data-sharing tools and interoperable systems are fundamental to move data across borders

Digital technologies offer new opportunities for people to share data and information, but interoperability is required to ensure that data can be used by different platforms and devices. Economic transactions that can lead to inclusive growth are increasingly dependent on data being transferred across the world. Data may be gathered from different sources and for different purposes, and combined in various ways to create value.[89] For people and societies to truly benefit from the digital era, digital products and services should be able to connect. This is not only about extracting value in a commercial sense, but also about using data to power tools and services (such as healthcare or financial services) that can better serve people. Shared and open standards can enable interoperability, compatibility, and consistency across markets.[90] Microservices, application programming interfaces (APIs), civic digital infrastructure, and other forms of interoperability reduce the costs and simplify the creation of new digital services.[91]

There are strong arguments supporting data interoperability for both economic and social gains. Giving consumers control over their personal data can generate allocations that are close to optimal and address privacy considerations. People should be able to easily move information about themselves across platforms and services, balancing their concerns for privacy against the gains emerging from the use of data.[92] Also, because the use of data is a factor of production across multiple firms, and data can be used many times without losing its value (in economic jargon, one would say data is *nonrival)*, portability increases its economic efficiency.[93] Research shows that standardisation and interoperability between different mobile payment systems is crucial to the development of new and innovative mobile money solutions in developing countries. Open standards on such systems foster consumer mobility (by reducing switching costs) and competition between mobile network operators, leading to more incentives to innovate.[94]

In practical terms, data sharing and portability should be reasonably achievable for most large companies. Even though the nature of data ownership currently remains rather unclear, most multinational firms already make data available to individuals on request.[95] In the same way as the incompatibility of electrical appliances can be solved with plug adapters, incompatibility of software and platforms can be mediated by 'digital adapters', which enable data portability. There are already public and private initiatives that champion data portability, which provide different frameworks for user control and consent. Google, Facebook, Microsoft, Twitter, and Apple are developing the Data Transfer Project, an open-source initiative to enable seamless, direct, user-initiated portability of data between different platforms. Other products such as Digi.me – a service that aggregates, normalises and structures data from different apps and services to make it easily reusable – aims to give users fine-grained control over who has access to their data. There are also examples of similar systems in the public sector. The government of India offers a service called DigiLocker, which provides a cloud account for every Indian citizen to access their official documents and certificates, such as their driving licence, voter ID, and school certificates, in digital format.[96] Other examples of interoperability are APIs and 'microservices', which reduce the costs of digital services, by making them accessible for further use, innovation, and integration within a broader ecosystem of digital services.

International coordination might be required to ensure data portability and interoperability. Technical and regulatory standards that work for different countries need to be in place to allow frictionless movement of data across borders. Interesting tools provided by private companies, as discussed above, can only go so far. However, it can be difficult for resource-constrained governments to develop and manage such tools alone. Furthermore, if each country develops unique standards, this will severely limit the market and scalability of any new digital product. International standardisation – of the sort championed by groups like ID4D – is an important part of seizing the gains from digital integration.[97] For example, each country could develop their own digital ID, but ideally, they would need to be at least partially interoperable. In practice, the structure could be similar to that of an hourglass: the bottom and the top represent the range of different systems and models each country could adopt, while the narrow middle would represent a basic shared standard, a checkpoint at which the variety of systems would be easily readable and interoperable.[98]

Box 2. **Measuring the value of digital transactions**

Data has a value that might not be visible when one does not 'pay' for services: people may not realise that there is value in an exchange involving sharing personal information if there is no price attached to it. Different studies have tried to measure the value of data, applying different methods to do so.[99] Data as 'the new oil' is often an imprecise and unhelpful analogy. Oil, as a natural resource, is measurable, tangible, limited, and strictly regulated.

In contrast, to date, there are no effective metrics or tools to assess the value of the intangible assets that power the digital economy (eg algorithms and data), making it difficult to compare the effects of global policies across different contexts. This matter is increasingly important: as the world becomes more and more digitised and data-driven, the ability to accurately value intangible assets will be all the more important for economic growth and investment. Indeed, in parts of the world, intangible assets reportedly now account for up to one-third of production value – or some US$5.9 trillion in 2014 – across 19 manufacturing industries.[100]

Intangible assets are particularly hard to evaluate because their value ultimately depends on a business or government's ability to use them – the same database may have vastly different 'value' to different firms. Furthermore, many intangible assets may be used across borders, making it even more difficult to quantify their value. Available data on international trade mostly comes from developed countries, and often does not clearly distinguish between the domestic and cross-border elements of transactions. This adds to the problem for developing countries, as it may cause significant errors in valuations for investments.

It should be noted that not all data is the same. Different types of data are collected and used in varying ways in different industries. Raw, unstructured data is rarely as valuable as data employed to solve a problem – the application determines the value of data. The amount of data and the size of the database are also relevant. Large, aggregated datasets are usually more valuable than individual sets of personal data (although there might be diminishing returns from big data sets) – the average person's data is reported to be worth less than a dollar on secondary markets.[101]

Efforts to measure the digital economy have been led by initiatives like the OECD/G20 working group and the Task Force on International Trade Statistics (TFITS), as well as the United Nations Conference on Trade and Development (UNCTAD), the International Monetary Fund (IMF), the World Intellectual Property Organization (WIPO), and the World Bank Group.[102] Developing countries should have a seat at these fora to ensure that the outcomes reflect their interests and priorities. In any case, the sharing of the value of cross-border data flows would require a negotiation that recognises the source of this value, and enables developing countries to capture their fair share.[103]

Further investigation would be needed to develop indicators to detect a business's remote but sustained and significant involvement in the economy of a market jurisdiction. Some proxy measures could take supply-and-demand factors into account, such as digital sales and number of users. This would be relevant for successful implementation of a global tax and accurately identifying relevant global markets. Ultimately, to meet growing policy needs, the development of a flexible, simple data typology, digital economy measures, and metrics and statistics, will be increasingly relevant.

Chapter 3
The case for regional and international coordination

Current approaches to governing, managing, and regulating digital technology do not help developing countries: now is the time to set this right. These emerging global norms are largely predicated around the interests and needs of rich nations. Even though regional approaches to technology governance are starting to emerge, developing countries individually have little ability to shape international rules, or to implement their own technology governance frameworks. Regulation of the digital economy will continue to grow in importance on the global agenda, and the resultant governance mechanisms will be pivotal for those seeking to make the most of the opportunities on offer. While global institutions remain dominated by larger, richer nations, international coordination – through regional or other voluntary groupings – presents developing countries with an opportunity to exercise their voices and develop a governance model that works for them, especially where their interests align. This chapter will set out the challenges faced by developing countries in the international governance of technology, to make a case for international coordination in their interests.

As social and economic life becomes increasingly digitalised, effective regulation and governance of the digital world is becoming fundamentally important. The number of people connected to the internet in developing countries is growing rapidly, although starting from a relatively low base. Half the world remains offline, but for those who are connected, digital products and services make up an increasingly important part of life, from transferring money by SMS to job-hunting on social media. Digital tools are also enabling entirely new industrial pathways, such as labour platforms for the informal economy (eg motorcycle taxi apps) or increasing the value from agriculture (eg through better analytics and supply chain management).[104] The business models and digital architectures designed by firms can have far-reaching impacts, and these are inherently shaped by the regulatory environment.[105] And yet, surprisingly little attention is paid to how poorer or resource-constrained countries should approach digital regulation. Good governance of technology can help countries harness the benefits of digital transformation, whereas inaction can leave citizens and domestic industries on the back foot, left behind in a global revolution.

The problems raised by digitalisation – the problems that policymakers feel compelled to solve – are largely a matter of domestic policy, but their causes are anything but domestic. Citizens' rights to privacy, competition between firms, security and law enforcement, business taxation; all of these matters traditionally fall within the remit of the nation state, rather than the web of international intergovernmental institutions. But digital firms operate across borders at almost no marginal cost, and their lack of physical presence in developing countries renders enforcement of jurisdiction and local regulations difficult. While many people in a given country might interact with a digital firm, that firm can operate with no office or physical activity within the country, making it difficult to enforce any governance regime. Such problems have a precursor in analogue challenges, such as taxation of multinational companies (as we discussed in Chapter 2), but the increasingly digital nature of business means that they are now emerging on a much greater scale.

At the global level, we can see new norms beginning to take shape around digital governance and regulation.[106] Indeed, a multipolar governance architecture is emerging, with the US, EU and China as global leaders.[107] In reality, a more nuanced view includes other countries – eg India and Estonia – establishing unique approaches. However, the multipolar global view remains a useful frame for analysis. The EU's GDPR provides a good example of the influence of these global leaders. It covers a broad range of issues, from consent to the management and security of personal data, and these have already been adapted into corresponding policies by non-EU countries such as the Philippines and Brazil.[108] Indeed, the Council of Europe's Convention 108 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – termed 'GDPR lite' by some) has 55 members, with Argentina, Cabo Verde, Mexico and Morocco joining in 2018 and 2019.[109] The US, meanwhile, currently operates a patchwork of state and federal laws, but these constitute the implicit default for many digital firms originating in the US.[110] Other approaches include China's 'great firewall', a popular term that obscures the breadth of China's approach to digital regulation, which has essentially led to a splintered version of the internet created for the Chinese context.[111] And indeed, parts of China's approach are going global, with Nigeria and Tanzania both implementing cybersecurity laws that mirror those of Beijing.[112] Policies from these major actors can quickly become de facto international standards. The influence of global powers also extends to infrastructure, as they are also developing competing – and often incompatible – technological stacks: programming languages, frameworks, software, and other tools. The states that write these rules and develop such architectures are thus given immense power: as other countries choose to mirror these standards, complex technical and regulatory interdependencies are formed, over which developing countries have little control.[113] Moreover, as interactions between these three influential powers – the US, the EU, and China – become inevitable, it will be necessary to harmonise their policies in some way.

Developing countries have a relatively limited set of regulatory options in the face of emerging global trends. The emerging global standards may not be suitable for every country, whether because they have different values (between, say, national security and business freedom), different sizes and populations, or simply because they do not have the capacity to enforce these regulatory models. But the alternative to these standards – developing a local regulatory approach – is not always an option. Most developing countries represent very small markets, contributing negligible revenue to large multinational firms.[114] These states may be able to regulate their homegrown domestic digital firms, but should their rules deviate too far from the de facto global standards and require too much compliance effort, we can expect global firms to simply exit. As a survey respondent pointed out, 'setting standards to enable interoperability, building indigenous capacity, infrastructure, and public-private-partnerships with technology companies are all things that can use international partnerships, because the West is ahead in this area and many of these innovations have come and the tech companies are from the West'. It is highly unlikely that a firm would go to the effort of complying with more than 100 unique – and possibly contradictory – regulatory regimes. Indeed, this is partly why China's great firewall spawned a whole ecosystem of Chinese internet companies: firms like Google refused to comply with China's regulations, opening a gap for Chinese search engine Baidu to establish itself.[115] Smaller countries know they have little power to directly regulate these firms, and this affects their regulatory options. This leads to approaches like Uganda's tax on social media users (see Box 1), or Papua New Guinea's temporary block of Facebook.[116] However, developing countries should not lose hope: in aggregate, they still represent a significant market. Indeed, India has been able to effectively write its own regulations because it is large enough – for example, Box 1 describes India's unique approach to taxing non-resident digital firms.

Global governance – such as that through the UN and its institutions – is a slow process, and developing country perspectives are often under-represented. A recent UN panel on digital cooperation presented a clear vision for strengthening multilateralism, multi-stakeholderism and diversification of voices in further digital cooperation. However, subsequent processes will take many years to result in global approaches to the (largely domestic) policy questions discussed in this paper.[117] In the consultation described earlier in this paper, policymakers in developing countries stressed that, with regards to digital governance, regulatory and technical standards are the two most important things they currently need from the international community. In the instances where multilateral treaties have been developed to establish such standards, developing countries are usually left out – for example, the Budapest Convention on Cybercrime, which now has 66 signatories, was drawn up by the Council of Europe.[118] And where global institutions already exist, they often do an imperfect job of representing the interests of developing countries, due to structural issues such as vote shares, as well as from informal norms.[119] While smaller, regional, and more representative groupings are increasingly addressing technology policy, most global fora tend to be dominated by the same small number of powerful actors behind emerging international regulatory norms –

a feature of their general geopolitical power. As for purely technical bodies, these civil society organisations were formed by early internet pioneers (computer professionals, academics, industry leaders), based mainly in the US, at a time when the internet had no regard for nation states and geography. As a result, neither do their governance structures, which almost all lack geographic or political representation.[120]

International coordination between developing countries offers a possible solution. In the face of a global regulatory environment shaped by a few powerful countries – which, in many cases, do not even share the same priorities and have competing interests – smaller nations are left without much agency. They cannot act unilaterally to forge their own rules, and they cannot expect inter-governmental institutions to respond quickly in protecting their interests. However, if developing countries pool their resources, capacity, and economic and political clout, they have the opportunity to define their own governance. Regional and sub-regional fora, for example, have the potential to amplify the voices of smaller countries, as such groupings will represent larger populations and markets than any one country alone. For example, there is an increasing consensus in the EU that the establishment of minimum requirements on cybersecurity must be undertaken at the EU, rather than national, level.[121] However, such groups need not necessarily be regional: coordinated groups may increasingly be based on shared interests and ideologies, as opposed to geographical proximity. Although it is clear that the current, institutional global models of multilateralism offer limited hope for change, acting together in new multilateral groupings may be the only way for developing countries to have their say in digital technology governance. The next chapter will consider specific actions and areas for cooperation between developing countries in the digital sphere.

Chapter 4
Principles for international coordination

The intangible nature of digital technology means that many issues span across borders, demanding some level of coordination. Chapter 2 discussed the priorities seen in the results of the Pathways for Prosperity consultation, which laid out the major concerns from the developing countries' perspectives. For each of the six key issues, there are different options and interests to be considered by policymakers and regulators. Countries must decide for themselves where they stand, based on their specific context and goals. Chapter 3 argued that with international coordination, developing countries can clear a few common hurdles that prevent action on these issues. In that chapter, we saw how developing countries have little power to unilaterally impose regulations on multinational firms. Even if they did, they often lack bureaucratic capacity to develop their own technology governance regimes.

This chapter identifies how the identified policy challenges could be addressed, offering principles for coordinated international action that speak to developing country concerns. As we have seen, many of the priority concerns emerging from the consultation are already being shaped by factors outside a nation's control. However, as discussed in Chapter 3, emerging trends in the governance of technology are authored by a small number of powerful countries; the priorities of developing countries do not drive these discussions. The five principles discussed here aim to shift the debate towards international cooperation that can work in countries with varied institutional capacities and support developing countries in harnessing the opportunities of digitalisation. Some of these principles are inherently cross-border, while others could have both domestic and international approaches. They provide ideas as to how countries can join together in efforts to navigate the digital age, but implementing them will present challenges: in all cases, they will require consideration of trade-offs and complex negotiations with all relevant stakeholders.

4.1 Foster digital cooperation: creating incentives for countries to work together

The challenges of digitalisation offer developing countries the opportunity to champion regional and international cooperation mechanisms that will work for them. In Chapter 2, we explored many technology policy issues that are priorities for developing countries. It may be too early to say which of the many policy options are the best for them. Indeed, this is partly because many developing countries are holding back, waiting to see if an international approach will emerge. However, global institutions are unlikely to solve the problems of digitalisation for the poorest countries. Intense rivalries between the major players mean that a consensus is unlikely to emerge any time soon.

Developing countries can chart their own paths towards international cooperation, finding an uncomplicated point of agreement they can use to start to build trust. There are policy areas in which countries can more easily start to work together, areas around which there is less disagreement within the international community. The incentives for coordination over digital policy will be stronger in areas where cross-border spillovers are more immediate, or where the efficiency gains from acting together are greater – for example, in addressing the online harms mentioned in Chapter 2.[122] Countries already have strong incentives to collaborate to tackle cybercrimes (eg child pornography), and addressing this issue could be a gateway to forge cooperation in other areas. To follow this example, tackling cybercrime would require bilateral and regional agreements to share information, institutions to oversee cross-border collaboration, and standards and procedures for information sharing, among other measures.

In practice, this could be implemented through a progressive process: once developing countries have identified their policy priorities and objectives, they can consider how international coordination might support their efforts. From there, they can look for like-minded partners to forge collaborations, and assess the best way to do so (regionally, multilaterally, globally, established institutions, new institutions, and so on). Once those systems are in place, developing countries could benefit from established coordination and cooperation mechanisms and use the same 'backbone' to address more contentious issues, where incentives would be harder to align – such as taxation and distribution of the value attributed to digital goods. Peer learning and sharing experiences is a good way to open channels for cooperation. The consultation showed a common theme amongst developing country policymakers: the need for international coordination to foster peer learning. One survey participant reported that 'sharing good practices is one of the actions that would be very useful for the policymaking process', while another said that 'international action is required to provide information and knowledge on the latest innovations and their functionality'. The importance of sharing practices also emerged from the Pathways for Prosperity Commission's in-country engagements, piloting its **Digital Economy Kit**,[123] where discussions with stakeholders revealed the relevance and importance of peer learning.

4.2 Tailor digital governance for developing countries: better ensuring implementation in a wider range of national contexts

Global standards governing digital technology may not be a good fit for developing countries, which have particular constraints and policy goals that often differ from those faced by developed nations. As outlined in the previous chapters, most developing countries have little scope to unilaterally design rules governing the digital economy: being relatively small markets, they must stay fairly close to de facto global standards (such as the EU's GDPR or the US regime for privacy and data protection). Standards come in many different forms, including product standards, codes of conducts and labels, and distinct types of process standards.[124] But many global standards governing digital technologies may be ill-suited to developing country contexts, especially when they are created by and in the context of developed nations. In some cases, developing countries lack the capacity to implement and enforce highly detailed regulations. In other cases, these emerging global standards may clash with other policy goals (for instance: they may limit investment).[125]

Any multi-country rule or standard should adopt a tiered approach that would allow developing countries to determine for themselves the best regulatory arrangements for their domestic and regional digital economy. This will include rules that address the issues discussed in the previous chapters. For example, in the financial sector, there is a growing understanding that, to maximise the stability benefits for developing countries, Basel III standards need to be adapted to match their unique needs and capacities – the so-called 'proportional application' of the standards.[126] In order for the best policy design to endure, developing countries should coordinate to pool their political clout and their resources. However, our research and consultation have highlighted a major recurrent concern: the cost of implementing, monitoring, and enforcing new regulations that are highly technical in nature. For this reason, any rule or standard that spans across borders should consider a tiered approach, starting with a minimum-implementable baseline that any country could (reasonably) be expected to meet in order to join an integrated digital market. From there, further tiers of regulation would be optional (see Box 3 for more detail). As discussed in the previous section, it would be easier to start with groups of countries that share similar values and objectives, for example, within regional or sub-regional groups – illustrated by the case of the electronic ID in the EU, discussed in Box 3.

The proposed tiered approach would involve built-in mechanisms to give countries incentives to move to another tier at a later stage. From a spectrum of compatible options, developing countries must decide for themselves where their available resources should be concentrated and they must assess the relevant trade-offs. For example, the standard-setting body that deals with anti-money laundering has introduced proportionality to address different capabilities.[127] While countries opting for the less stringent tiers would be subject to a lower regulatory burden, they would also be subjected to limitations in terms of the activities they could perform. In such a scenario, countries would have to weigh the costs of compliance against the benefits of having access to a given market. This would be similar to debates in trade in which countries can self-declare as least developed countries (LDCs), but are restricted in terms of the transactions with which they can engage.[128]

Box 3. **A tiered approach to cross-border rule-making**

A concrete way to think about differentiated standards would be a tiered approach. An initial, starting tier would have minimum requirements, which may still be challenging to meet where experience and funding are lacking. Countries in this tier should also receive support to develop their own local capacities. To prevent forum-shopping, the lower regulatory requirements would come with greater limitations for cross-border transactions.

Countries could then move to a middle tier, which would require them to adopt further conditions, but still enjoy some regulatory leeway. This intermediary tier would also provide its countries – and companies based within them – with greater licence to participate in the connected global economy.

Once countries have developed the learning and institutional capacity to fully comply with high regulatory standards, they could move into the final tier and be subject to stringent requirements around specific policy topics, with unfettered market access.

For example, a specific agreement regulating digital data sharing for law enforcement purposes could require countries to have adequate levels of data protection in place to receive overseas information. Country A, which does not have any such rules in place, could join the agreement in its lower tier, whereby it would have access to information only through a secured system, and the amount of information available would be limited. Once country A passes regulation establishing a certain level of data protection, it could then move to a higher tier and have access to a greater volume of information. When the country fully complies with the data security requirements of the agreement, it would have direct access to data for partner countries, and would be able to transfer and process the information in its own jurisdiction.

There are examples of similar approaches already in practice. In 2014, the EU introduced an electronic identification regulation (eIDAS), which establishes different levels of assurance (low, substantial, and high), according to the degree of confidence in a given ID scheme – ie how accurate the system is in identifying a given person. Establishing the level of assurance takes into account processes (eg identity proofing, verification, and authentication), management activities (eg the entity issuing electronic identification and the procedure to issue such means), and the technical controls implemented. The premise is that this would improve trust amongst member countries regarding electronic identification and remove barriers to the cross-border use of online services within the European single market.[129]

4.3 Unlock data for inclusive development: using data to improve people's lives

Data portability and the right to access data can unlock its value for citizens and policymakers. The consultation highlighted a perceived conflict between the goals of spurring economic growth and improving data governance.[130] While this concern might be legitimate in some cases, it should not spark a regulatory race-to-the-bottom to attract international firms. When data is governed well, countries can unlock its immense power to solve local problems. The world's information can be classified into different types of data, depending on how it was collected and who or what it relates to: personal or non-personal, sensitive or non-sensitive, to name a few.[131] Much of this information is locked away in proprietary databases and is only used for a slim fraction of its possible applications. Unlocking this data does not need to be at the expense of either privacy or safety: in fact, these are complementary goals that – in increasing trust and people's willingness to share data – enhance the potential benefits of data use.

Ensuring that people have the right to access and use their data for their benefit can unlock new and innovative applications of data for inclusive growth. Global debates about digital regulation are often reduced to a dichotomy between an EU-style 'privacy first' choice, or a US-style laissez-faire choice, although the reality is of course more nuanced.[132] Developing countries, however, can consider alternative frameworks that account for additional policy goals: responsible governance with an eye to fostering nascent industries and new innovations. Ensuring people the right of access to data that relates directly to them, along with simple tools for portability (meaning people can choose to use platforms aligned with their needs), will be important in unlocking this potential. Users need to be able to see their personal data and to access it in a commonly used and machine-readable format. A basic principle that underlies this idea is that, if the information directly relates to a person, that person should be able to access and use the data, even if they did not collect it.

There are alternative (non-mutually exclusive) policy options to unlock the data for inclusive growth. For example, one possible approach could be a proportionate progressive policy. In such a scenario, small data holders would still be required to grant users access to their personal data, but would be exempt from more burdensome requirements. As firms' revenues or user bases grow, they could be progressively compelled to respond to more complex data requests from users and communities, including making data available in a machine-readable format, making aggregate, anonymised data available through an API, and making community-scale data available to policymakers. Other approaches include requiring firms to make data available in certain formats, or requiring data to be shared in a controlled environment, accessible to other approved businesses or organisations.[133] Governments or other bodies could also act as trustees of such data as a social resource, stipulating conditions about its use and how it should be 'mined' in the public interest.[134]

This approach could also extend to pieces of information that are not personal data, such as traffic data, satellite imagery, crop yields, or water flows. Personal data does deserve special attention and additional security measures, but there is a whole world of data to be explored that does not fall within this category.[135] In fact, aggregated data and metadata could be even more useful from a public policy perspective. That said, compelling – for example – a satellite firm to share images with a community for free could damage the satellite imagery business, if that community sells the data on to a competitor. If the business model breaks, then no one will benefit from the data. This concern could be reduced through non-commercial requirements (prohibiting data recipients from re-selling) or instead making the initial data access possible at a 'fair price', rather than for free. There are distinct public benefits to using such data: big data and analytics are already playing an increasing role in transforming public services. For example, the app Strava uses aggregate data from runners and cyclists to help assess and shape transport policy in 76 cities around the world, through its spin-off company Strava Metro. In a similar initiative, Uber provides aggregate insights on traffic in a public dataset and partners with local policymakers to improve urban planning.[136]

Getting the most out of data will often require building capacity and investing in infrastructures that favour portability and further uses of data. Given the non-rivalrous nature of data (ie the same data can be used multiple times without losing its value), there are clear benefits to enhancing access to it and facilitating reuse.[137] However, data sharing has yet to reach its potential, in part due to lack of capacity and a limited awareness of how to maximise the potential social and economic values of data. To complement the alternatives listed above, investments in education and research are needed and should be considered in development support. This could include, for example, requiring that data used in research is openly available for further use, or labelling datasets as public goods. This is especially important for government-funded research, but private donors could also consider funding training and capacity building to enhance access to data and to support the development of public databases.

4.4 Be part of something bigger: harmonising cross-border digital trade

The digital economy is increasingly dependent on data being transferred across different locations, systems and devices. However, integration is not without its issues (as discussed in Chapter 2). Many countries are starting to reject deep international digital integration, often on the grounds of economic or law enforcement concerns. However, far from being a problem, harmonising cross-border trade can actually support significant new industries. The more integrated these systems and markets are, the faster, cheaper, and more reliable it will be for entrepreneurs to create new products, and for consumers to access affordable services. Similar efforts led by regional organisations are already underway, such as the United Nations Economic Commission for Latin America and the Caribbean (ECLAC) 2020 digital agenda for Latin America and the Caribbean (eLAC), the Digital ASEAN Initiative, and UNECA's Digital Transformation Strategy for Africa. Another concrete example of policies to further integration is the Policy and Regulation Initiative for Digital Africa (PRIDA), which aims to create a more harmonised and enabling legal and regulatory framework across Africa, and to strengthen cooperation between national telecommunications regulatory authorities across the continent.[138]

The economic benefits of removing barriers to the cross-border flow of data cannot be ignored when weighing the trade-offs involved in the regulation of technology. One of the rationales for restricting or regulating the flow of data is political: these regulations are often the only ones with teeth for countries contending with large multinational technology firms, and thus their only available bargaining chips. Another rationale is economic: to promote the domestic development of the IT industry. Rejecting digital integration (say, by pursuing data localisation or data sovereignty rules) is often seen as a means to kick-start domestic industry.[139] However, there is a trade-off when restricting data flows, for economic reasons: recent analysis suggests that restricted data flows will make countries less attractive to investors, have limited positive effects on the local industry, and may raise costs for local entrepreneurs.[140] In fact, failing to share data may ultimately stifle economic growth and lead to increased prices and decreased productivity in industries that depend intensively on data services (Box 4 contains a further discussion on the geography of data storage).[141] If countries pursue this approach, it may be worth negotiating built-in review mechanisms, such as a 'sunset' clause, to assess the effects of the regulation, and eventually remove it at a later date. Further, if barriers to data flows are established, a coordinated bloc of developing countries could explicitly exempt each other, creating a south-south network of open digital trade among countries with similar regulatory standards. One survey participant from Latin America highlighted the advantages of integration:

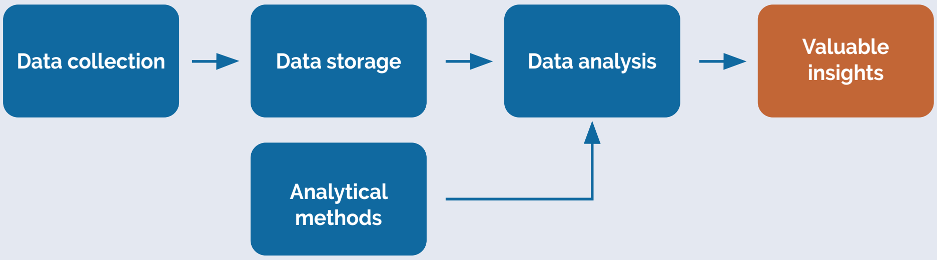
> **'harmonisation through standards and international treaties may bring benefits, but tends to be hugely detrimental to developing nations, due to the imbalance of power in international negotiations… south – south cooperation would be the most interesting kind of action'.**
> Survey respondent

Box 4. **The geography of data: economic and social value from using data**

The geography of data – where it is physically stored and processed – is beginning to play a role in policy debates. But in analysing these concerns, it is important to distinguish between the different steps of the digital value chain. Physical storage may not turn out to be so important.

Data is only valuable when it is analysed to produce useful insights, for instance, about consumer preferences (in the advertising industry) or demographic distribution (in the health sector). Looking along the value chain, the data must first be collected, perhaps by a social media app or a community service provider. It is then processed and stored on a server. Later, it is picked back up and combined with an analytical method to produce insights. Because it is relatively frictionless to move data between places and across borders, each of these stages can occur anywhere. They are geographically agnostic.

Figure 5. **A simplified diagram of the data value chain – each of these stages could occur in a different country**



The middle stage in this chain – the physical storage of data – is a commodity input. With the advent of large-scale cloud computing, small- and medium-scale data storage is a globally competitive market. Many countries are considering broad data localisation laws that would require firms that collect local data to store that data on local servers. These laws are often explicitly framed in economic terms, reasoning that keeping the data within the country's borders will ensure that the value generated from the data will stay within the country.[142] But as we discuss in Box 2, it is not so simple to assume that data has an intrinsic value.

The value accrues to the organisation that processes or analyses data for profit – regardless of where the data is stored. If a US digital advertising firm is forced to store its data on a local server, then it will pay commodity prices for server space, and this small amount of value will be retained locally. Indeed, the real value is created when the firm runs their proprietary algorithms to target consumers, and then sells that service for a profit. There is nothing to say that this revenue and profit will be used locally.

There can be some benefits to local data storage. It makes sense to store certain pieces of information locally, such as data that relates to national security. It also makes sense to store these on a custom secure system, not commodity-level cloud servers. Mandated localisation could also make sense if a country wanted to protect (or to kick-start) a local data warehouse industry that would otherwise be uncompetitive against the cloud giants. This would likely create jobs for warehouse builders and server maintenance staff, perhaps creating a first step for human capital development. There are also incentives for governments to leverage localisation policies in the context of negotiations. In many cases, this is the only available move against large companies which hold most of the power.

However, for countries that truly want to cultivate innovative and strong digital ecosystems, there is more value in trying to foster firms at the final stage of the ecosystem: those that develop novel analytical methods and good business models for data use. For firms engaged in this sort of business, data localisation will actually impose a cost: requiring them to pay more for a commodity input (data storage), rather than buying it in a competitive global market.

Rather than being merely a challenge, facilitating cross-border digital trade could help to address policy priorities in a more inclusive way. Integration and adoption of shared standards would facilitate access to data, as well as coordination and information sharing among law enforcement authorities, making it easier for agents and authorities to access and act on data that is relevant to their work. As previously discussed, greater data mobility and open systems are the building blocks of interoperability, which can enhance market competition and benefits for consumers.[143] Consistent standards in areas such as micro-payments and digital identities can supercharge innovation. For example, a standard open banking API can make it much easier to start an e-commerce business.

4.5 Protect against cyber harms: establish data protection, transparency, and accountability measures

International coordination can help to protect countries from digital harms such as data breaches and algorithmic discrimination. Citizens, governments, and businesses need to feel safe to invest and take part in the integrated digital market (discussed in the previous section). If the appropriate safeguards are not in place, removing barriers to data flows and providing the technical scaffolding to enable connections might not be enough to unlatch cross-border digital transactions.

Establishing clear rules and data protection requirements can help to build trust amongst stakeholders. There are three broad areas in which a coordinated governance approach can help governments protect users and society alike: data collection; storage and transfer; and processing. For example, companies would need to trust that their confidential data is protected when storing it on an overseas cloud service provider, and users need to feel safe to share their personal data when using an e-government service. Solutions usually involve some combination of consent, transparency and data security requirements – including guidelines about the conditions under which data is stored and transferred.[144]

Throughout the consultation, policymakers also expressed uncertainty about the growing use of machine learning and other artificial intelligence tools. This was one of the policy issues most survey participants expected to face in the coming years.[145] Mounting evidence shows that automated systems can discriminate against more vulnerable groups and worsen existing injustices.[146] These technologies are having a significant impact in developing countries, where they are being applied in some fields even before they are applied in rich nations (for example, automated credit assessments for people without a credit score). As the use of automated mechanisms by governments and companies increases, the need to understand how decisions are made and the accuracy of the results also grows. Some jurisdictions are therefore moving towards the idea that algorithms be 'interpretable' by humans.[147] Whether this represents best practice is an open debate: some argue it is burdensome on firms, precludes the use of many promising machine-learning techniques, and may risk the leakage of trade secrets.[148] Other approaches could include giving people the choice to opt-out of 'high-risk inferences' (where decision-making processes could damage their privacy or reputation),[149] or using non-discrimination regulations (with means of redress) to make firms liable if their algorithmic decisions are found to unfairly discriminate against groups or individuals based on their faith, gender, race or ethnicity, for example.[150]

Most developing countries do not have clear regulatory regimes that deal with these issues. At the international level, there is only a patchwork of approaches to data governance. As more and more information exists in digital form, the risks also grow. Now is the appropriate time to consider shared norms and rules to protect users and societies from potential harms. The poorest and most resource-constrained countries would naturally require more support in such efforts. While funding and capacity building remain key modes of international support in the digital age, the international community can also go further. Pursuing shared rules and standards through a coordinated international or regional bloc would reduce the risk of multinational firms being put off by fragmented and uncoordinated regulation; increasing legal certainty and likely fostering investment between member countries. Having a coordinated response seems preferable to a scenario in which each developing country builds its own 'data realm', and its own rules of the game.[151] Such regulations would establish an opt-in tiered approach, which could be well suited to the needs, priorities, and resources of developing countries.

Chapter 5
Conclusion

This paper has discussed how policy issues that prevent developing countries from harnessing the opportunities of new technologies are not merely questions of domestic policy, but also require concerted international cooperation. The Pathways for Prosperity consultation with policymakers, government officials, entrepreneurs, and global technology experts revealed that many pressing concerns of the digital age – including taxation, cybercrime and cybersecurity, privacy and data protection, intellectual property, and data sharing and interoperability – will require significant cross-border collaboration. In the words of one of the survey respondents:

> **'While I am certain that [my country] can achieve its technology policy goals on its own, this may take a much longer period of time without international coordination. The latter has the ability and capacity to keep the dialogue alive through stakeholder engagements and forums for discussions, and through arranging peer pressure to galvanise action.'**
> Survey respondent

While it is clear that the international community needs to take action to help developing countries capitalise on technological progress, there is still uncertainty as to what the appropriate institutional framework should look like. As discussed in Chapter 3, poorer countries are traditionally underrepresented and unable to make their voices heard amidst the dominant voices of 'great powers' in multilateral governance institutions. There have been attempts to bring more representation to many of these fora, and regional blocs have been championing important initiatives. However, in many ways, multilateralism is under strain and it is still not clear how formal institutions will be the genesis of governance solutions. Many countries are actively pursuing national domestic policies, rather than multilateral coordination, for a range of issues – not just digital governance. Furthermore, solving the complex problems discussed in this paper – such as digital taxation or competition policy – will not only be a matter of political coordination. Many of the current best-practice frameworks for regulation are strained by the digitalisation of the economy. Without new technical approaches to regulation that address these emerging strains, there are likely to be missed opportunities for inclusive development.

Any long-term solution to these issues will likely require a rethinking of the role and mandate of international bodies, but there are ways developing countries can start working together now. Developing countries cannot wait for global institutions to solve these problems, or for richer nations to decide on the best way to distribute the value from data. Instead, they can leverage their digital assets and start developing their own models of cross-border regulation that work for them. The five principles discussed in this paper can be viewed as a guide towards a more integrated digital world. But to be clear: this is unlikely to be an all-encompassing framework from day one – countries will not be able to solve multinational taxation in all its complexities using this framework. Pursuing such principles will require working diplomatically, engaging with multiple stakeholders, and addressing competing interests. Developing countries need to take charge of technology governance to better tailor it to their own businesses, society, and economy. While this agenda presents many challenges, it provides a starting point for cooperation – which can begin today.

References

Aaronson, S. A. (2018). *Data Is Different: Why the World Needs a New Approach to Governing Cross-Border Data Flows*, CIGI Paper No. 197. Series: CIGI Papers Series.

Abbott, F. M. (2014). 'Trade Costs and Shadow Benefits: EU Economic Partnership Agreements as Models for Progressive Development of International IP Law'. In J Drexl, HG Ruse-Khan and S Nadde-Phlix (eds) *EU Bilateral Trade Agreements and Intellectual Property: For Better or Worse?* 20:159–70. Berlin, Heidelberg: Springer.

African Union (2017). *Policy and Regulation Initiative for Digital Africa (PRIDA).* [Online] Available at: www.africa-eu-partnership.org/en/projects/policy-and-regulation-initiative-digital-africa-prida [Accessed 13 Sep. 2019].

African Union (2019a). *African Union Convention on Cyber Security and Personal Data Protection.*

African Union (2019b). *African Leaders Redefine the Future through Digital Transformation*. Available at: https://au.int/en/pressreleases/20190211/african-leaders-redefine-future-through-digital-transformation

Agam, H. (1999). 'Equitable Geographic Representation in the Twenty-first Century'. In Thakur, R. (1999) *What is Equitable Geographic Representation in the Twenty-first Century*. Tokyo: United Nations University.

Akileswaran K., and Hutchinson, G. (2019). *Adapting to the 4IR: Africa's development in the age of automation.* London: Tony Blair Institute for Global Change.

Azmeh, S. and Foster, C. (2016). *The TPP and the digital trade agenda: Digital industrial policy and Silicon Valley's influence on new trade agreements*. LSE Department of International Development. Working Paper Series 2016. London: London School of Economics and Political Science.

Bansal, S., Bruno, P., Denecker, O., Goparaju, M. and Niederkorn, M. (2018). Global Payments Map 2018, *Global payments 2018: A dynamic industry continues to break new ground*. Global Banking, October 2018. New York: McKinsey & Company.

Barron, L. (2018). *Papua New Guinea Is Planning to Shutdown Access to Facebook for One Month, Report Says. Time.* [Online]. Available at: https://time.com/5294869/papua-new-guinea-facebook-shutdown/ [Accessed 29 Jul. 2019].

Basu, A., Hickok, E. and Chawla, A. S. (2019). *The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India*. India: The Centre for Internet & Society.

Bauer, M., Ferracane, M. F., and Marel, E. (2016). 'Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization'. Paper Series: No. 30 – May 2016. Global Commission on Internet Governance. Ontario: Centre for International Governance Innovation (CIGI) and Chatham House.

Beaton-Wells, C. (2019). 'Competition in the Digital Economy: New Realities, New Thinking'. Keynote presentation at the UNCTAD Intergovernmental Group of Experts on Competition Law and Policy, Geneva, 10 July 2019.

Beck, T. and Rojas-Suarez, L. (2019). *Making Basel III Work for Emerging Markets and Developing Economies*. Washington, DC: Center for Global Development.

Bhasin, M. L. (2016). Privacy Protection Legislative Scenario in Select Countries: An Exploratory Study. *International Journal of Management Sciences and Business Research*, Oct-2016 ISSN (2226–8235) Vol-5, Issue 10.

Bopanna, A. (2018). ICANN Diversity Analysis. Domlur, India: Centre for Internet & Society (CIS). Available at: https://cis-india.org/internet-governance/blog/icann-diversity-analysis [Accessed 13 Sep. 2019].

Brannon, I. and Schwartz, H. (2018). 'The New Perils of Data Localization Rules'. *Regulation,*vol. 41, no. 2, Summer 2018, pp. 12–13.

Bundeskartellamt (2019). Bundeskartellamt obtains far-reaching improvements in the terms of business for sellers on Amazon's online marketplaces. [Press release, 17 July, 2019]. Available at: www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/17_07_2019_Amazon.html%3Bjsessionid=3FA24E906F055630261D46840A52D193.1_cid378?nn=3591568 [Accessed 13 Sep. 2019].

Caribou Digital (2018). *Identity at the margins: Identification systems for refugees*. Surrey, UK: Caribou Digital Publishing.

Carter, W. A., and Yayboke, E. (2019). *Data Governance Principles for the Global Digital Economy.* Washington DC: Center for Strategic and International Studies (CSIS).

Casado, M. and Lauten, P. (2019). *The Empty Promise of Data Moats*. California: Andreessen Horowitz. Available at: https://a16z.com/2019/05/09/data-network-effects-moats [Accessed 13 Sep. 2019].

Castelluccia, C. and Métayer, D. (2019). *Understanding algorithmic decision-making: Opportunities and challenges*. European Parliamentary Research Service (EPRS).

Chenou, J-M. (2014). From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-stakeholderism, and the Institutionalisation of Internet Governance in the 1990s. *Globalizations* Vol 11, 205-223.

Ciuriak, D. (2019a). 'Unpacking the Valuation of Data in the Data-Driven Economy'. *SSRN*.

Ciuriak, D. (2019b). *World Trade Organization 2.0: Reforming Multilateral Trade Rules for the Digital Age*. Waterloo: Centre for International Governance Innovation (CIGI).

Ciuriak, D. and Ptashkina, M. (2019). *Leveraging the Digital Transformation for Development: A Global South Strategy for the Data-Driven Economy*. Waterloo: Centre for International Governance Innovation (CIGI).

Clifford Chance (2019). *The OECD proposal to revolutionise worldwide taxation: Our assessment*. London: Clifford Chance. Available at: www.cliffordchance.com/briefings/2019/06/the_oecd_proposaltorevolutioniseworldwid.html [Accessed 13 Sep. 2019].

CMA (2018). *Pricing algorithms research, collusion and personalised pricing*. London: Competition and Markets Authority.

Cook, C. (2018). Cross-Border Data Access and Active Cyber Defense: Assessing Legislative Options for a New International Cybersecurity Rulebook. *Stanford Law & Policy Review* 29, no. 2: 33.

Council of Europe (2019a). *Chart of signatures and ratifications of Treaty 108*. [Online] Available at: www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=p03PYqXg [Accessed 13 Sep. 2019].

Council of Europe (2019b). *Chart of signatures and ratifications of Treaty 185*. [Online] Available at: www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=Pl6UfUHu [Accessed 13 Sep. 2019].

Coyle, D. (2018). *Practical Competition Policy Implications of Digital Platforms*. Working paper n. 01/2018. Cambridge: Bennett Institute for Public Policy.

Crivelli, E., De Mooij, R., and Keen, M. (2015). *Base Erosion, Profit Shifting and Developing Countries*. IMF Working Paper, 29 May, 2015. Washington: International Monetary Fund.

CSIS (2018). *China's Emerging Data Privacy System and GDPR*. Washington: Center for Strategic and International Studies.

CSIS and McAfee (2018). *Economic Impact of Cybercrime – No Slowing Down*. Washington: Centre for Strategic and International Studies.

Daskal, J. (2016). Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues. *Journal of National Security Law & Policy,* 8, no. 3: 31.

Daskal, J. (2019). Privacy and Security Across Borders. *Yale Law Journal* 128 (2019).

de La Chapelle, B. and Fehlinger, P. (2016). *Jurisdiction on the internet: from legal arms race to transnational cooperation*. Paper Series: No. 28 – April 2016. Ontario: Centre for International Governance Innovation.

de Sousa Abreu (2018). Disrupting the disruptive: Making sense of app blocking in Brazil. *Internet Policy Review*, 7(3).

Devereux, M. P. and Vella, J. (2018). Debate: Implications of Digitalization for International Corporate Tax Reform, *Intertax*, Issue 6/7, pp. 550–559.

Drahos, P. (2005). Developing Countries and International Intellectual Property Standard-Setting. *The Journal of World Intellectual Property*, no. 5, pp. 765–89.

European Union (2014). *EU Regulation No 910/2014 (eIDAS Regulation).* [Online] Available at: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Legislation+in+a+nutshell [Accessed 13 Sep. 2019].

Ezrachi, A. and Stucke, M. (2016). *Virtual Competition*. Massachusetts: Harvard University Press.

Facebook (2019). *Will I be charged tax on my purchases of Facebook ads?*. [Online] Available at: www.facebook.com/business/help/133076073434794 [Accessed 13 Sep. 2019].

Farrell, H. and Newman, A. L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security*, v. 44, issue 1, p.42–79.

FATF (2017). *Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion*. Paris: Financial Action Task Force.

Ferreira, C., Jenkinson, N. and Wilson, C. (2019). *From Basel I to Basel III: Sequencing Implementation in Developing Economies*. Washington: International Monetary Fund.

Fox, E. M., and Bakhoum, M. (2019). *Making Markets Work for Africa: Markets, Development, and Competition Law in Sub-Saharan Africa*. Oxford: Oxford University Press.

Furman et al (2019). *Unlocking digital competition: Report of the Digital Competition Panel*. London: HM Treasury.

G7 (2019). *Chair's summary: G7 Finance Ministers and Central Bank Governors*. Biarritz: G7 France.

Geller, E. (2018). *China, EU seize control of the world's cyber agenda*. POLITICO. [Online] Available at: www.politico.eu/article/china-eu-dominate-cyber-agenda-us-on-tech-sidelines/ [Accessed 13 Sep. 2019].

Ghorbani, A. and You, J. Y. (2019). *What is your data worth? Equitable Valuation of Data*.

Goldfarb, A. and Tucker, C. (2012). Privacy and Innovation. *Innovation Policy and the Economy.* National Bureau of Economic Research, Chicago: University of Chicago Press.

Google (n.d.a). *Google Cloud Global Locations – Regions & Zones*. [Online] Available at: https://cloud.google.com/about/locations/?region=asia-pacific#region [Accessed 13 Sep. 2019].

Google (n.d.b) GO-JEK: Using Machine Learning for forecasting and dynamic pricing. Available at: https://cloud.google.com/customers/go-jek/ [Accessed 13 Sep. 2019].

Government of India (2016)*. Government of India's Finance Act 2016*, Chapter VIII.

Government of India (2018). *Framing of Income-tax rules relating to Significant Economic Presence as per Section 9(1)(i) of the Income-tax Act, 1961*. Ministry of Finance.

Government of Vietnam (2013). *Decree No. 72/2013/ ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information*.

Greenleaf, G. (2016). *Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives*. (2016) 142 Privacy Laws & Business International Report,14–17; UNSW Law Research Paper No. 17–3.

Greenleaf, G. (2019). *Global Data Privacy Laws 2019: 132 National Laws & Many Bills*. Privacy Laws & Business International Report, 14–18.

Gruber, H. (2019). Proposals for a digital industrial policy for Europe,*Telecommunications Policy,* 43(2), pp. 116–127.

Gupta, V. (forthcoming).*Taxation on Cross-Border Electronic Transmissions: Policy Options for Developing Countries*. Pathways for Prosperity Commission Background Paper Series. Oxford, UK: Pathways for Prosperity Commission.

Haskel, J. and Westlake, S. (2018). *Capitalism without Capital: The Rise of the Intangible Economy*. Princeton, New Jersey: Princeton University Press.

Hassan, E., Yaqub, O. and Diepeveen, S. (2010). *Intellectual property and developing countries: A review of the literature.* Cambridge: Rand Europe.

Hernández Rathe, L. M. (2017). *Entry into force of Law No. 42–08 on Defense of Competition in the Dominican Republic: Immediate Practical Consequences*. Latin America Legal [Online]. Available at: www.latlegal.com/2017/03/entry-into-force-of-law-no-42–08-on-defense-of-competition-in-the-dominican-republic-immediate-practical-consequences/ [Accessed 13 Sep. 2019].

Hoffmann, A. L. (2019). Where Fairness Fails: Data, Algorithms, and the Limits of Antidiscrimination Discourse. *Information, Communication & Society* 22, no. 7 (7 June 2019): 900–915.

Hoffmann, J., Bakhoum, M., and Beneke, F. (2018). *Digital Markets, Mobile Payments Systems and Development Competition Policy Implications in Developing Countries in Light of the EU Experience*. Max Planck Institute for Innovation & Competition Research Paper No. 18–13, 2018. Munich: Max Planck Institute for Innovation & Competition Research.

Ido, V. (2019). *Intellectual Property and Electronic Commerce: Proposals in the WTO and Policy Implications for Developing Countries*. South Centre Policy Brief No. 62, 8. Geneva: The South Centre.

IPA (2016). *Driving change: Australia's cities need a measured response*. Sydney: Infrastructure Partnership Australia.

ITU (2012). *Understanding cybercrime: Phenomena, challenges and legal response*. Geneva: International Telecommunication Union.

Jatania, B. (forthcoming). An Antitrust Approach for Regulating Zero-Price Digital Platforms in India. Mumbai, India: IDFC Institute.

Jones, C. I. and Tonetti, C. (2018). *Nonrivalry and the Economics of Data*. Working Paper No. 3716. California: Stanford Graduate Business School.

Jones, E. and Knaack, P. (2019). Global financial regulation: shortcomings and reform options. *Global Policy*, 10(2), 193–206.

Kalanje, C. M. (2006). *Role of intellectual property in innovation and new product development*. Geneva: World Intellectual Property Organization.

Kerber, W. (2016). Digital markets, data, and privacy: competition law, consumer law and data protection, *Journal of Intellectual Property Law & Practice*, Volume 11, Issue 11, 856–866.

Koene et al (2019). *A governance framework for algorithmic accountability and transparency.* Brussels: European Parliament Research Service.

Kumar, B.R. (2019). Bayer's Acquisition of Monsanto. In: *Wealth Creation in the World's Largest Mergers and Acquisitions*. Management for Professionals Series. Basel: Springer Nature Switzerland.

Lagarde, C. (2018). *Estimating Cyber Risk for the Financial Sector.* IMF Blog. [Online] Available at: https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/ [Accessed 13 Sep. 2019].

Lahiri, A. K., Ray, G. and Sengupta, D.P. (2017). *Equalisation Levy.* Brookings India Working Paper 02. New Delhi: Brookings Institution India Center.

Landau, S. (2015). Control use of data to protect privacy. *Science* 347.6221 (2015): 504–506.

Lee, J-A. (2018). *Great Firewall*: *The SAGE Encyclopedia of the Internet*, pp. 407–410. In Warf, B. (ed). (2018). *The Chinese University of Hong Kong Faculty of Law Research Paper No. 2018–10.*

Maillart, JB. (2019). The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime. *ERA Forum* 19, no. 3 (March 2019): 375–90.

Marotta-Wurgler, F. (2016). Self-regulation and competition in privacy policies. *The Journal of Legal Studies* 45.S2 (2016): S13-S39.

Manyika, J., Lund, S., Bughin, J., Woetzel, J., Stamenov, K.and Dhingra, D. (2016). *Digital Globalization: The New Era of Global Flows.* New York: McKinsey Global Institute.

Max Planck Institute for Innovation and Competition (2013). *Principles for intellectual property provisions in bilateral and regional agreements*. Munich: Max Planck Institute for Innovation and Competition.

Mayer, J. (2017). Government hacking. *Yale Law Journal*, 127. 570.

McDonald, S. (2019). Reclaiming Data Trusts. Centre for International Governance Innovation (blog). [Online] Available at: www.cigionline.org/articles/reclaiming-data-trusts [Accessed 13 Sep. 2019].

McDonald, S. and Mina, X. (2018). War-Torn Web: A once unified world has broken into new warring states. *Foreign Policy*. [Online] Available at: https://foreignpolicy.com/2018/12/19/the-war-torn-web-internet-warring-states-cyber-espionage/#map [Accessed 13 Sep. 2019].

McGowan, K., Vora, P., Homer, M. and Dolan, J. (2018). *Personal data empowerment: restoring power to the people in a digital age*. Pathways for Prosperity Commission Background Paper Series; no. 11. Oxford, UK: Pathways for Prosperity Commission.

Menell, P. S. (2017). Rise of the API Copyright Dead: An Updated Epitaph for Copyright Protection of Network and Functional Features of Computer Software. *Harvard Journal of Law & Technology*. 3, p. 305.

Misra, P. (2019). *Lesson from Aadhaar: Analog aspects of digital governance shouldn't be overlooked*. Pathways for Prosperity Commission Background Paper Series; no. 19. Oxford, UK: Pathways for Prosperity Commission.

Moerland, A. (2017). Do Developing Countries Have a Say? Bilateral and Regional Intellectual Property Negotiations with the EU. *IIC – International Review of Intellectual Property and Competition Law*, 48, no. 7, pp. 760–83.

Moore, M. and Prichard, W. (2017). *How Can Governments of Low-Income Countries Collect More Tax Revenue?*. ICTD Working Paper 70. Brighton, UK: International Centre for Tax and Development, Institute of Development Studies (IDS).

Morin, J. F. and Thériault, D. (2019). *Copyright Provisions in Trade Deals: A Bird's-Eye View*. CIGI Policy Brief No. 149, May 2019. Waterloo, Canada: Centre for International Governance Innovation.

Muhammad, A. et al (2019). Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Skewed Outcomes. *ArXiv:1904.02095 [Cs]*, 3 April 2019. New York: Cornell University.

Nadvi, K. (2008). Global standards, global governance and the organization of global value chains. *Journal of Economic Geography*, Volume 8, Issue 3, May 2008, Pages 323–343.

OECD (2014a). *Addressing the Tax Challenges of the Digital Economy*. OECD/G20 Base Erosion and Profit Shifting Project. Paris: OECD.

OECD (2014b). *Challenges of International Co-operation in Competition Law Enforcement.* Paris: OECD.

OECD (2014c). *Measuring the Digital Economy: A New Perspective*. Paris: OECD.

OECD (2019). *Members of the OECD/G20 Inclusive Framework on BEPS.* Paris: OECD.

OECD and G20 (2016). *Towards a G20 initiative on measuring Digital Trade: mapping challenges and framing the way forward.* Paris: OECD.

OECD and G20 (2019). *Programme of Work to Develop a Consensus Solution to the Tax Challenges Arising from the Digitalisation of the Economy*. OECD/G20 Inclusive Framework on BEPS. Paris: OECD.

Parliament of Uganda (2018). *Report on the Committee on Finance, Planning, and Economic Development on the excise duty (Amendment Bill, 2018).*

Pathways for Prosperity Commission. (2019a). *Positive disruption: health and education in a digital age*. Oxford, UK: Pathways for Prosperity Commission.

Pathways for Prosperity Commission (2019b). *Digital Economy Kit*. Oxford, UK: Pathways for Prosperity Commission.

Pathways for Prosperity Commission. (2018a). *Charting Pathways for Inclusive Growth: From Paralysis to Preparation*. Oxford, UK: Pathways for Prosperity Commission.

Pathways for Prosperity Commission. (2018b). *Digital Lives: Meaningful Connections for the Next 3 Billion*. Oxford, UK: Pathways for Prosperity Commission.

Phillips, T. (2019). *What data dominance really means, and how countries can compete*. World Economic Forum. [Online]. Available at: www.weforum.org/agenda/2019/02/what-data-dominance-really-means-and-how-countries-can-compete/ [Accessed 29 Jul. 2019].

Phillips, T., Kira, B., Dolan, J., Tartakowsky, A. and Natih, P. (forthcoming). *Digital technology governance: developing country priorities and concerns* (working title). Oxford, UK: Pathways for Prosperity Commission.

Pisa, M. and Polcari, J. (2019). *Governing Big Tech's Pursuit of the "Next Billion Users".* Washington: Center for Global Development.

Reinsel, D., Gantz, J., Rydning, J. (2018). *The Digitization of the World From Edge to Core.* IDC White Paper. Massachusetts: IDC.

Richards, N. M. (2013). The dangers of surveillance. *Harvard Law Review*, 126(7), 1934–1965.

Richter, H. and Slowinski, P. R. (2019). The Data Sharing Economy: On the Emergence of New Intermediaries, *International Review of Intellectual Property and Competition Law*, 50:4.

Ricketson, S. (1992). New wine into old bottles: Technological change and intellectual property rights. *Prometheus* 10.1 (1992): 53–82.

Schaub, F., Balebako, R. and Cranor, L. F. (2017). Designing effective privacy notices and controls. *IEEE Internet Computing*. Volume: 21, Issue: 3, May-June 2017.

Sheehan, M. (2018). How Google took on China – and lost. *MIT Technology Review.* [Online] Available at: www.technologyreview.com/s/612601/how-google-took-on-china-and-lost/ [Accessed 29 Jul. 2019].

Singh, P. J. (forthcoming). *Evolution of Global Digital Governance: A Southern View.* Pathways for Prosperity Commission Background Paper Series. Oxford, UK: Pathways for Prosperity Commission.

Singh, P. J. (2017a). *Digital Industrialisation in Developing Countries – A Review of the Business and Policy Landscape*. IT for Change.

Singh, P. J. (2017b). *Report on Developing Countries in the Emerging Global Digital Order*. IT for Change.

Srivats, K. (2019). Digital tax: Centre rakes in moolah with 'equalisation levy'. *The Hindu Business Line*. [Online] Available at: www.thehindubusinessline.com/economy/digital-tax-centre-rakes-in-moolah-with-equalisation-levy/article26260963.ece [Accessed 29 Jul. 2019].

Steel, E. (2013). Financial worth of data comes in at under a penny a piece. *Financial Times*. [Online] Available at: www.ft.com/content/3cb056c6-d343–11e2-b3ff-00144feab7de [Accessed 13 Sep. 2019].

Steel, E., Locke, C., Cadman, E. and Freese, B. (2013).How much is your personal data worth. *Financial Times*. [Online] Available at: https://ig.ft.com/how-much-is-your-personal-data-worth/#axzz2z2agBB6R [Accessed 13 Sep. 2019].

Stork, C. and Esselaar, S. (2018). *Unleash, Not Squeeze, Uganda's ICT Sector*. Vancouver: Research ICT Solutions.

Superintendencia de Industria y Comercio (2019). *Superindustria sanciona a Uber con $2.128 millones por obstruir visita administrativa*. [Online] Available at: www.sic.gov.co/Superindustria-sanciona-a-Uber-por-obstruir-visita-administrativa [Accessed 29 Jul. 2019].

Świątkowska, J. (forthcoming). *Unleashing digital potential of developing countries by pragmatically tackling cybercrime challenges*. Pathways for Prosperity Commission Background Paper Series. Oxford, UK: Pathways for Prosperity Commission.

Umaña, M. A. (2018). *Regional Competition Agreements: The Case of Latin American and the Caribbean*. 17th Global Forum on Competition on 29–30 November 2018. Geneva: OECD.

UNCTAD (2019a). *Competition Issues in the Digital Economy*. Intergovernmental Group of Experts on Competition Law and Policy, 18th session. Geneva: United Nations.

UNCTAD (2019b). *Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries*. Geneva: United Nations.

UNCTAD (n.d.) Data protection and privacy legislation worldwide. [Online] Available at: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx [Accessed 13 Sep. 2019].

United Nations (2019). The Age of Digital Interdependence. Report of the UN Secretary-General's High-level Panel on Digital Cooperation. Geneva: United Nations.

United Nations (n.d.) Trade-related international support measures (ISMS) for LDCS. [Online] Available at: www.un.org/ldcportal/category/trade-international-support-measures/ [Accessed 13 Sep. 2019].

UNODC (2013). *Comprehensive Study on Cybercrime*. New York: United Nations Office on Drugs and Crime.

US Department of State (2016). *Doing Business in Belize: 2016 Commercial Guide for U.S. Companies*.

Valente, M. G. (forthcoming). *IP, Global Technologies and the Research Arena*. Pathways for Prosperity Commission Background Paper Series. Oxford, UK: Pathways for Prosperity Commission.

Vestergaard, J. and Wade, R. H. (2013). Protecting power: how Western states retain the dominant voice in the World Bank's governance. *World Development*, 46. pp. 153–164.

Wachter, S. and Mittelstadt, B. (2018). A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI (October 5, 2018). *Columbia Business Law Review*, 2019(2).

WIPO (2017). *World Intellectual Property Report 2017: Intangible Capital in Global Value Chains*. Geneva: World Intellectual Property Organization.

Wolfram, S. (2019). Testimony before the US Senate on Optimizing for Engagement: Understanding the Use of Persuasive Technology on Internet Platforms.

Woods, N. and Domenico Lombardi, D. (2006). Uneven patterns of governance: how developing countries are represented in the IMF. *Review of International Political Economy.*

World Bank (2018). The Catalog of technical standards for digital identification systems. Available at: https://id4d.worldbank.org/technical-standards

Zittrain, J. (2019). Chapter 45 – Internet, In *A History of IP in 50 Objects.* Cambridge: Cambridge University Press.

Zuiderveen Borgesius, F. (2019). Algorithmic Decision-Making, Price Discrimination, and European Non-discrimination Law. *European Business Law Review.*

Zureik, E., Stalker, L. H., Smith, E., Lyon, D. and Chan, YE. (eds) (2010). *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*. Montreal: McGill-Queen's University Press.

Endnotes

[1] Phillips et al (forthcoming). The formal consultation process was conducted between February and August 2019.

[2] To ensure citizen buy-in and to balance digital with other national priorities, any developing country's approach to governance of technology should be conscious of capacity and the competing interests of multiple stakeholders. As the Pathways Commission argued with its Digital Economy Kit, when navigating the challenges of digitalisation, countries should convene broader social conversation, ensuring that all relevant groups are represented, especially the most marginalised ones. The Digital Economy Kit provides a framework to help developing countries identify which strategies might work for them and the relevant stakeholders to engage. Available at: https://pathwayscommission.bsg.ox.ac.uk/digital-toolkit/digital-economy-kit-0

[3] Reinsel et al. (2018).

[4] Pathways for Prosperity Commission (2018b).

[5] Bansal et al. (2018).

[6] Manyika et al. (2016).

[7] Pathways for Prosperity Commission (2018a).

[8] Microservices are digital services distilled to their simplest possible parts, and then packaged in a way that other developers can use in their applications. Microservices can often be bought for a comparatively low fee, saving digital service providers the time and expense of developing such services themselves. See Pathways for Prosperity Commission (2018a).

[9] Google (n.d.a).

[10] Google (n.d.b).

[11] UNCTAD (2019a).

[12] Based on the respondents who identified themselves as having expertise on a low- or middle-income country, according to the World Bank grouping.

[13] Phillips et al (forthcoming).

[14] For example, Uganda's social media tax (see Box 1) caused a drop in internet usage and imposed a heavy burden on the poorest internet users. See Pathways for Prosperity Commission (2018b) for a discussion of how options are limited for developing countries when it comes to regulating international digital service providers (p. 34).

[15] As argued by Singh (forthcoming), throughout the evolution of global digital governance, there have been several examples of cases in which developing countries' voices have been less heard in debates around technology.

[16] India has been in the spotlight for its recent experiences with policy and regulation of technology, such as the Aadhaar case (Misra, 2019).

[17] It is worth mentioning the centrality of data governance issues: when considering 'privacy and data protection' and 'data sharing and interoperability' together, the merged group ranks higher than jobs and skills (Pathways for Prosperity Commission, forthcoming).

[18] Devereux and Vella (2018).

[19] Crivelli, De Mooij, and Keen (2015).

[20] Gupta (forthcoming).

[21] Authors' calculations, based on the average per-country audience of Facebook's advertisements, as reported in its ads portal (Phillips, 2019).

[22] For example, Facebook ad purchases are subject to different value added tax (VAT) or goods and services tax (GST) rules, depending on the country where the advertiser is based. Some countries, such as India and Colombia, have clear rules governing taxation of digital transactions, while other developing countries still have not addressed the issue (Facebook, 2019).

[23] UNCTAD (2019b).

[24] OECD (2014a).

[25] For example, digital technologies can make it easier to identify and register potential taxpayers, who can easily stay out of the tax net, and can also introduce taxpayer services such as filing tax returns and paying tax bills online. See: Moore and Prichard (2017).

[26] As the Uganda example in Box 1 shows, taxes based on usage seem unlikely to work out well for most developing countries and can lead to poor distributional outcomes. The ability to tax multinationals on sales or transactions could be an alternative, even though there could also be worries about fairness if the tax is passed on to domestic residents.

[27] Parliament of Uganda (2018).

[28] OTT or 'over-the-top' subscriptions include video, audio or other media content (including internet-based audio calls and messaging) which circumvents traditional distribution channels such as broadcast and satellite television platforms.; Available at: https://twitter.com/UCC_Official/status/1088826918957404160

29 Stork and Esselaar (2018).

30 Government of India (2016).

31 Lahiri, Ray and Sengupta (2017).

32 Srivats (2019).

33 Government of India (2018).

34 OECD (2014b).

35 G7 (2019) and OECD (2019).

36 OECD and G20 (2019). This proposal, however, is likely to be controversial and cause disagreement regarding the formula and the base to which it is applied, in order to decide the proportion of profit generated by each country (for example, considering sales, assets and employees in each country). Clifford Chance (2019).

37 Lagarde (2018); CSIS and McAfee (2018).

38 UNODC (2013).

39 Maillart (2019).

40 Świątkowska (forthcoming).

41 ITU (2012).

42 For example, the African Union Convention on Cyber Security and Personal Data Protection was adopted in June 2014, but by August 2019, only 14 countries had signed it and five had ratified it. This prevents the convention from coming into force, as it has a minimum requirement of ratification by 15 countries. For the text of the treaty and the updated list of the countries, see African Union (2019a).

43 Pisa and Polcari (2019).

44 Government of Vietnam (2013).

45 Brannon and Schwartz (2018).

46 For a discussion of government hacking, see Mayer (2017). For a discussion of the dangers of surveillance, see Richards (2013).

47 Basu, Hickok, and Chawla (2019).

48 de La Chapelle and Fehlinger (2016), Cook (2018).

49 Daskal (2016).

50 For example, in Brazil, courts ordered the blockage of WhatsApp in the entire country for 72 hours when the company failed to provide law enforcement authorities with content of messages sent by an individual as part of a criminal investigation (de Sousa Abreu, 2018).

51 Daskal (2019).

52 For example, China's data protection regime and the EU's GDPR both provide protection against misuse of data but differ on matters such as definitions of consent and data processing. China's data protection regime is less restrictive than GDPR on issues such as consent and data processing, apparently in an effort to provide room for growth to emerging technologies, such as Artificial Intelligence (CSIS, 2018). This may stem from a difference in value ascribed to privacy in these two contexts: the Chinese social tradition of valuing collective good over individual good, along with its political system that administers tight control over citizen activities and records, sets a relatively low bar for individual privacy, compared to the European GDPR (Zureik et al, 2010).

53 UNCTAD's map that shows which countries have data protection laws (UNCTAD, n.d.).

54 Greenleaf (2019).

55 Phillips et al (forthcoming).

56 Bhasin (2016), Kerber (2016), Landau (2015), and Schaub, Balebako, and Cranor (2017).

57 Singh (2017a).

58 There is also a debate about the use of satellite and drone surveillance by humanitarian agencies to map migrant populations and to identify individuals. There is concern that refugees are rarely offered the opportunity to exercise control over what data is collected, despite having an interest in, and the capacity to do so (Caribou Digital, 2018).

59 Some digital rights activists have indeed argued that Europe should export the GDPR in order to encourage rights-based legislation elsewhere (Akileswaran and Hutchinson, 2019).

60 Goldfarb and Tucker (2012).

61 Bundeskartellamt (2019).

62 The definition of the relevant market (ie the sector and geography in which a company operates) is important in defining which businesses are competitors in a given market, but this is particularly difficult in the digital age. For example, Google and Facebook offer different services to users – one is a search engine, while the other is a social media platform. However, both can be considered competitors in the market for online advertising. (Coyle, 2018); (Jatania, forthcoming).

63 Ezrachi and Stucke (2016), see also CMA (2018).

64 UNCTAD (2019a).

65 UNCTAD (2019a). In some cases, competition authorities do not have enough information to reach an informed decision, and they encounter resistance from technology companies. For example, in Colombia, the antitrust regulator recently fined Uber nearly US$625,000, for allegedly obstructing an investigation into the company's operations in the country by preventing the regulators from accessing relevant documents (Superintendencia de Industria y Comercio, 2019).

66 For example, Belize (US Department of State, 2016) and Guatemala (Umaña, 2018).

67 Countries without competition law include Nigeria, Ghana, and Togo; see Fox and Bakhoum (2019); In the 1980s, many countries adopted principles established by the Washington Consensus and responded to pressure from the World Bank, spurring the development of competition law and policy in many developing countries since the 1990s (Fox and Bakhoum, 2019).

68 Hernández Rathe (2017).

69 Fox and Bakhoum (2019).

70 Pathways for Prosperity Commission (2018a).

71 UNCTAD (2019a).

72 UNCTAD (2019b).

73 OECD (2014c).

74 In July 2019, there were 66 cases worldwide investigating antitrust practices involving one of the big technology companies (Google, Amazon, Apple, and Facebook). To date, 27 policy studies addressing the particularities of digital markets have been published by regulators and competition authorities. Beaton-Wells (2019).

75 Fox and Bakhoum (2019).

76 Kumar (2019). In the digital space, the Uber-Grab merger is an example of a transaction that involves coordination between multiple competition authorities in South-East Asia (UNCTAD, 2019a).

77 Phillips et al (forthcoming).

78 Haskel and Westlake (2018).

79 Kalanje (2006).

80 Ricketson (1992).

81 Software is protectable under copyright, and this protection generally extends to written algorithms such as API implementing codes; Menell (2017); WIPO (2017).

82 Hassan, Yaqub and Diepeveen (2010).

83 Drahos (2005).

84 Valente (forthcoming).

85 Ido (2019).

86 Valente (forthcoming).

87 For more on this, see Moerland (2017), Max Planck Institute for Innovation and Competition (2013), Abbott (2014), and Morin and Theriault (2019).

88 Moerland (2017).

89 OECD (2014c).

90 Furman et al (2019).

91 Pathways for Prosperity Commission (2019a).

92 Of course, there are non-economic uses of data, as we will discuss in section 4.3.

93 Jones and Tonetti (2018).

94 Hoffmann, Bakhoum and Beneke (2018).

95 Self-regulation arrangements can increase willingness to share data by addressing technical and legal concerns. Richter and Slowinski (2019).

96 The African Union (AU) and the United Nations Economic Commission for Africa (UNECA) have been working on a Digital Transformation Strategy for Africa, which also contains the Digital ID, to some extent inspired by the Indian experience (African Union, 2019b).

97 World Bank (2018).

98 The hourglass analogy is often used to describe the architecture of the internet: where the physical layer with cables, transmissor, and receptors at the bottom, and a wide range of services, content, and applications on the top, and the TCP/IP standard at narrow middle (Zittrain, 2019).

99 For example, Ghorbani and You (2019) propose a framework to address data valuation in the context of supervised machine learning. The *Financial Times* built a calculator that allows one to check the worth of an individual's personal data (FT, n.d.). Dan Ciuriak (2019a) proposed that the value of data should be captured in market capitalisation of data-intensive firms.

100 WIPO (2017). However, as recognised by WIPO, it remains to be established who ultimately gains this income, due to the difficulty of associating assets and earnings with a particular country location.

101 Casado and Lauten (2019); FT (2013).

102 OECD and G20 (2016); UNCTAD (2019b).

103 Ciuriak (2019b).

104 Pathways for Prosperity Commission (2018a).

105 Pathways for Prosperity Commission (2018b).

106 McGowan, Vora, Homer and Dolan (2018).

107 McDonald and Mina (2018).

108 Greenleaf (2019).

109 Greenleaf (2016). For a full list of countries, see Council of Europe (2019a).

110 McGowan, Vora, Homer and Dolan (2018).

111 Lee (2018).

112 Geller (2018).

113 Farrell and Newman (2019).

114 Phillips (2019).

115 This is not necessarily a replicable strategy for establishing local digital industries. China succeeded in part because they had the domestic skills and resources to replicate the companies they were blocking out, and also because they had the right economies of scale to support a local search engine or social media product (due to the size of its population). For more on the relationship between China and Google, see: Sheehan (2018).

116 Barron (2018).

117 UN (2019).

118 The Budapest Convention was drawn up by the Council of Europe. Although some developing countries, including South Africa, Sri Lanka, Panama and the Philippines have subsequently signed or ratified the Convention, they had no say in the development of its terms. See Council of Europe (2019b).

119 This is documented in a long-standing body of literature. See: Woods and Lombardi (2006); Agam (1999); and Vestergaard and Wade (2013).

120 See Chenou (2014) for more on this. Since those early days, the Internet Corporation for Assigned Names and Numbers (ICANN) in particular has made concerted efforts to broaden its stakeholdership and now has formal geographic representation. Also, a recent analysis conducted by the Center for Internet and Society finds that ICANN's mailing list (where various governance issues are discussed) is still overly dominated by industry stakeholders from the US. Their analysis notes that, 'Only 14.7% of the participants were from Asia, which is concerning since 48.7% of internet users worldwide belong to Asia.' (Bopanna, 2018).

121 Gruber (2019).

122 Pisa and Polcari (2019).

123 Pathways for Prosperity (2019b).

124 Nadvi (2008).

125 Singh (2017b).

126 Jones and Knaack (2019); Beck and Rojas-Suarez (2019); Ferreira, Jenkinson and Wilson (2019).

127 FATF (2017).

128 UN (n.d.).

129 EU (2014).

130 Phillips et al (forthcoming).

131 UNCTAD (2019b).

132 McGowan, Vora, Homer and Dolan (2018). It is worth mentioning that, in many cases, in the absence of formal laws, rules developed by private companies (eg privacy policies of internet platforms) play a relevant role in establishing the rights and limitations of users. See Marotta-Wurgler (2016).

133 Furman et al (2019).

134 This could be done, for example, through the establishment of legal trusts that manage data, or the rights to data. See McDonald (2019).

135 Aaronson (2018).

136 The platform is called Uber Movement. One example is the partnership between Uber Movement and the Infrastructure Partnerships Australia (IPA), whereby Uber Movement provided data to monitor the impact of planning and infrastructure decisions on real journey times in Melbourne, Sydney, Perth and Brisbane (IPA, 2016).

137 Jones and Tonetti (2018).

138 African Union (2017).

139 Azmeh and Foster (2016).

140 Brannon and Schwartz (2018).

141 Jones and Tonetti (2018), Bauer, Ferracane, and Marel (2016).

142 For instance, a proposal from India referred to the need for data localisation to help foster a local artificial intelligence industry. See: Basu, Hickok, and Chawla (2019).

143 Furman et al (2019).

144 Carter and Yayboke (2019).

145 Phillips et al (forthcoming).

146 See, for example, Muhammad et al. (2019); Hoffmann (2019).

147 Castelluccia and Métayer (2019) and Koene et al (2019).

148 Wolfram (2019).

149 Wachter and Mittelstadt (2018).

150 Zuiderveen Borgesius (2019).

151 Ciuriak and Ptashkina (2019).

Pathways
for Prosperity
Commission
*Technology &
Inclusive Development*

BLAVATNIK
SCHOOL OF
GOVERNMENT

UNIVERSITY OF
OXFORD