Australia Indonesia Partnership
for Economic Governance

KPPU
KOMISI
PENGAWAS
PERSAINGAN
USAHA

The Digital Economy in Indonesia

27 December 2017

Preface

This report provides an overview of some important digital economy issues in Indonesia. The report was commissioned by the Commission for the Supervision of Business Competition (KPPU) as part of the Technical Cooperation Agreement with the Australia Indonesia Partnership for Economic Governance (AIPEG) to promote Effective Competition Policy.

The report attempts to understand some of the emerging, digital economy issues in Indonesia and their impact on competition. It explains how digital services contribute to economic growth and employment, identifies key issues that may arise from the delivery of digital services, provides examples of Indonesia's approach to the issue, provides best practices from international organisations and different countries in approaching the issue and identify strategies to promote the digital economy.

Consultations were undertaken with a wide range of experts with an interest in Indonesia's digital economy. Some key stakeholders included the KPPU, the Ministry of Trade, the Financial Services Authority (OJK), other government ministries and agencies, the private sector and associations.

It is hoped that this report will be a useful guide for the KPPU and the Government of Indonesia in developing its response to the ongoing emergence of the digital economy.

AIPEG prepared this report with valuable assistance from the KPPU. AIPEG is grateful to the KPPU and all other persons who provided input into the preparation of this report.

Table of Contents

1. Overview

1.1 The Digital Economy

The digital economy can be described as a range of economic and social activities that rely upon or use IP-enabled networks and platforms as part of the embedded infrastructure of society.[1] It includes activities such as buying and selling, banking, and accessing education or entertainment using the Internet or connected devices.[2]

The challenge for policy makers has come from the rapid development of the digital economy as new technologies have enabled a wide variety of new entrants and new business practices to emerge. What is noteworthy is the impact that this is having on industries and businesses *across all sectors,* including: finance; transport; logistics and delivery; retail; insurance; healthcare; education; agriculture and aquaculture; manufacturing; energy; tourism and so on.

On the positive side, the digital economy stands to substantially boost economic growth and employment opportunities – in particular new work arrangements facilitated by digital technologies – as well as social inclusion, and therefore development. Online platforms, for example, have the potential to capture and agglomerate informal employment, employ inactive ("idle") parts of the population, and therefore reduce unemployment.

In Indonesia, as elsewhere, the strategic and widespread use of digital technologies, including social media and ecommerce, has the potential to have significant economic impact, including:

- Creating an additional 3.7 million jobs by 2025;[3]
- Generating up to 80% higher growth in revenue for small and medium enterprises (SMEs);[4] and
- Adding an additional 2% per annum in GDP growth by increasing broadband penetration rates and usage of digital technologies by SMEs.[5]

In 2015, ecommerce was estimated by Google and Temasek to have contributed USD1.7 billion to Indonesia's economy.[6] By 2020, the Indonesian government has targeted that ecommerce will have grown to USD130 billion. As long as the appropriate and coordinated regulatory frameworks are established, data (the "oil" of the digital economy) is able to flow both domestically and internationally, and the unintended consequences of poor policy making are avoided.

An overarching challenge for Indonesia's digital economy is the existence of overlapping mandates between various regulators and policy agencies which stands to confuse stakeholders and can complicate the implementation of clear and consistent regulatory

[1] TRPC, Going Digital: The Status and Future Potential of Internet-Based Economies in Asia (2015), p. 3
[2] Australian Government, The Digital Economy: Opening up the conversation (September 2017), p. 9
[3] Mckinsey&Company, Unlocking Indonesia's Digital Opportunity (2016), p. 15 https://www.mckinsey.com/~/media/McKinsey%20Offices/Indonesia/PDFs/Unlocking-Indonesias-digital-opportunity.ashx
[4] Deloitte Access Economics, SMEs powering Indonesia's success (2015), p. 3
[5] Deloitte Access Economics, SMEs powering Indonesia's success (2015), p. 1
[6] Google & Temasek, e-conomy SEA: Unlocking the $200 billion digital opportunity in Southeast Asia (September 2016), p. 10

frameworks. This challenge is not unique to Indonesia: digital technologies increasingly cut across regulatory areas of responsibility and can impact industries from all sectors of societies. Putting together an effective framework not only requires effective policy leadership, but also effective communication and coordination *across* regulators and relevant government agencies on an ongoing basis. Where to focus in bringing regulators together is thus as important as putting together a roadmap of prioritized action steps.

1.2 Scope of the Report

This report is meant as an initial identification and overview of key issues in the digital economy resulting from digital disruption, including:

- Markets and the emergence of new business models;
- Investment requirements (including into the base infrastructure) and challenges;
- Network management (and so-called “net neutrality”);
- Competition and consumer protection;
- Issues of data protection and data security; and
- Data localisation.

In each of the subsequent sections, we highlight the key development drivers of each issue, and the potential economic impact. Where applicable, we have identified how the issue is being addressed in Indonesia, such as current or proposed regulatory policy. We then highlight what good international practice looks like, and provide some brief examples of how this has been implemented in other jurisdictions.

1.3 Key Points

- Digital technologies are disrupting and transforming traditional markets and business models. As the boundaries between industries blur, the basis of competition changes.
- In the emerging digital economy, governments, including competition authorities, must address the challenges of protecting and empowering consumers in a complex and rapidly developing online environment, while enabling growth in the business environment.
- A prominent argument from traditional service providers, however, is that an “uneven playing field” is emerging as digital service providers are not subject to similar regulations governing their operations or their content.
- Regulation of digital services and service providers is challenging as regulators must determine whether there is a basis for regulation; whether regulation will restrict market entry; and whether regulation is practical and enforceable.
- If regulation is overly prescriptive it can stifle innovation, drive up costs, and restrict the growth of the Indonesian economy.
- From a competition perspective, the issue is whether the barriers to entry prevent competition, and whether they are “natural” or induced, for example, by anti-competitive practices or by exclusive licenses.
- Any regulatory framework should be forward-looking and flexible in order to keep pace with and benefit from technological advances. New frameworks should seek to *reduce* barriers to market entry, while remaining conscious of providing consumer protection, and surety of rules, regulations and responsibilities for organisations.

- To underpin the digital economy and enhance trust, a coherent data protection framework is required. Any data protection framework will need to be flexible to further enable innovation.
- The economic and social benefits of data flows, including increased market access, investment, innovation, development and growth, and an increase in productivity, are best realised when there are no data residency restrictions.

2. Markets and Business Models

2.1 Issue Overview

Digital technologies are in the process of disrupting and transforming traditional markets and business models. Examples include:

- **Online platforms** that enable the exchange of information, goods and services, disintermediating vertically integrated supply chains and fostering new "platform economy" business models. These include ecommerce and transaction providers, as well as purveyors of gig and sharing economy businesses.
- **Over-the-top (OTT)** services that utilise the existing telecommunications or communications infrastructure to establish a direct relationship between the service provider and the end-customer – who has downloaded the service provider's app to a device – no matter the location. These increasingly encompass all types of business, from the well-known such as Uber and Go-Jek, to heath care providers, banking services, and remote learning access services. Indeed, healthcare and banking services can now be provided without the need for building new physical infrastructure, or having practitioners or service personnel on location – or even in the same country.

Disruptive innovations are a natural consequence of technological evolution. As technology transforms how companies can operate and provide their services (and increasingly goods) to customers, innovative new business models emerge disrupting the market environment. Traditional definitions of industries and of sectors are increasingly under challenge as a result. Technology enables companies to expand across different sectors and provide their services to customers in a variety of industries. But the application of legislation, and importantly the framing of competition, is currently based on sectoral definitions; increasingly this does not reflect the way in which consumers perceive the services they consume.

This brings into question how governments and societies are organized and the way in which value is created. The example of Uber is often cited, but the impact is neither company nor sector specific. Service providers such as Uber, Didi, Grab, and Airbnb, bring into question what *type* of companies they are: are they taxi and hotel firms, transportation and hospitality businesses, or are they just software companies? Are they *platforms*? Is the driver of an Uber car an Uber employee or self-employed? Such designations can have profound implications for how the tax system and social security system works.

These developments are also transforming business models. In particular, digital economy business models are challenging our concept of "the uneconomic citizen": i.e., someone for whom the cost of connectivity, of being put onto the network, is not justified because of the perceived "meagre" economic returns to the connectivity provider. With the communications networks now a "horizontal" enabler and not simply a "vertical" sector, the benefits generated from providing someone with network access include the education, healthcare and broader participative (voting, welfare dissemination, tax, etc.) rights that accrue from that connectivity.

This is because interoperability of networked platforms can enable an increasing array of services delivery: e-education, e-government, e-health, and so on, and in so doing transform almost all sectors, including agriculture; aquaculture; energy; logistics; and transportation.

A key consideration for regulators in approaching disruption is to determine *the nature of the markets* in which companies operate, and to understand how their business models work in those markets and how they differ from those of traditional service providers. Further, regulators must consider how traditional service providers are responding and changing their own business and delivery models.

Regulation of digital services and service providers is thus challenging from several points of view:

- on what ground (and within which sector) the regulation is justified;
- whether regulations deter new entrants and stifle innovation; and
- whether regulation is practical and enforceable given (a) the speed with which new technologies and business models evolve, and (b) that digital services cut across both different sectors and different jurisdictions.

Over-the-top (OTT) Services Delivery

OTT services can be defined as digital content distributed over the Internet that bypass traditional communication delivery channels to reach end users, and that can potentially complement, collaborate or supplant not only traditional telecoms and media services but also a whole range of traditional industries.

OTT service categories are expanding at a meteoric rate and will often overlap, but for the purposes of conceptualizing they can be distilled down to:

- those that compete with traditional telecom services;
- those that compete with traditional broadcast services; and
- downloads and apps that offer new categories of service, ranging from downloads of music, games, maps, timetables, etc., to sharing-apps, informational apps, e-commerce apps, etc.

OTTs are often perceived by sector incumbents to have reduced the market share and revenues of traditional telecom providers and broadcasters. Given the expansion in services offered and the overall value being generated from the provision of such services, this is a rather simplistic or narrow interpretation, at best.

OTT services have certainly changed the operating environment of traditional licensed operators and service providers. Traditional operators express concerns that OTT service providers are not subject to the same regulations and policy restrictions as they are, for example, in terms of the collection and use of customer data, or content restrictions, and because they are unlicensed they pay no license fees despite competing in many of the same markets.

2.2 Markets and Business Models in Indonesia

As elsewhere, digital service providers in Indonesia are disrupting traditional business models. Local retail firm Matahari, for example, has begun closing outlets in Jakarta, and putting more resource and focus into its ecommerce ventures. Another example, Go-Jek, began by providing motorcycle taxi rides in Indonesia. Within three years, the operation had grown to

300,000 drivers earning an average of IDR4 million (USD296) per month – double the minimum wage. Significantly, having started out with ride sharing services, the company has used the same platform to provide an increasing multitude of other services that "share" under-used access to idle resources, including Go-Food, Go-Massage, Go-Glam, and most recently payment services through Go-Pay. So, while the traditional taxi companies are now competing with the digital "ride sharing apps", providing consumers with more choice and better service, has this "levelled the playing field" and are we talking about the same type of service? Should the taxi companies, such as Blue Bird, that have entered the digital space, creating their own customer-oriented apps to compete, now be classified as OTT companies, rather than taxi companies? Or should they be burdened with being regulated under both frameworks? Such an approach would result in high administrative costs for companies if they *are* required to apply for multiple different types of licenses for separate categories.

Examples worth citing go beyond the merely commercial: In recent Jakarta gubernatorial elections, technology supported the pursuit of clean governance through the use of a mobile application, *MataRakyat.*[7] Developed by PT InTouch, the app provided verification of vote counts by coordinating reporting mechanisms from witnesses across 13,000 polling stations, with a remarkably low 0.03% discrepancy ratio.

Notable examples of the recent creation and expansion of digital services in Indonesia include:

- **Go-Jek** (www.go-jek.com), an online platform providing on-demand services. Go-Jek has expanded its product offerings across verticals, including transport, food delivery, courier services and logistics, shopping deliveries, and mobile payments. This diversification has disrupted business models and markets across a number of sectors.
- **Tokopedia** (www.tokopedia.com), a consumer-to-consumer (C2C) online marketplace. Tokopedia is one of the largest ecommerce marketplaces in Indonesia. Some five million individuals and businesses in Indonesia manage their own online store on the platform, capitalising on shared resources and reducing their own business running costs.
- **Traveloka** (www.traveloka.com)**,** an online travel agency. Traveloka is Indonesia's top eticketing marketplace, capitalising in particular on the boom in business travel in Indonesia.
- **Ralali** (www.ralali.com), a business-to-business (B2B) online marketplace. Ralali connects buyers and suppliers by providing a one-stop shop for industrial supplies and maintenance, repair, and operational equipment. The ecommerce platform brings together around 50,000 unique product listings, which has made the procurement processes more transparent for consumers.

Recently proposed regulations by the Indonesian government, such as an ecommerce roadmap and draft OTT regulations, illustrate the dilemmas of regulating the changing markets and business models of digital service providers and traditional service providers.

[7] The Jakarta Post, Mobile app promises alternative election quick count (January 2017), http://www.thejakartapost.com/news/2017/01/18/mobile-app-promises-alternative-election-quick-count.html

Ecommerce Roadmap

A Presidential Regulation on the Roadmap for the National Ecommerce System 2017-2019 was released in August 2017.[8] The roadmap provides guidelines for Indonesia's digital economy sector and in so doing regulates various technologies, covering further issues such as logistics, cybersecurity, taxation, human resources development and consumer protection. The roadmap also prioritises the development of the National Payment Gateway (NPG).

Draft OTT Regulation

Indonesia is proposing to go further than most countries in regulating OTT services. An OTT draft regulation, released by the Ministry of Communications and Information Technology (Kominfo) in July 2017, requires that OTT players register their taxpayer ID number, principle license from the investment agency BKPM, types of OTT services that will be provided, and contact information centre details. The OTT service provider would also be required to partner with a national telecommunications entity.

The draft regulation defines an OTT operator by the following:

- **Application Services** through the Internet is the utilisation of software that enables communication services in the form of short messages, voice calls, video calls, emails, and online conversations (chatting), financial and commercial transactions, digital platforms, storage and retrieval of data, search engines, game, networking and social media, as well as its derivatives that use Internet access services through telecommunication network providers.
- **Content Services** over the Internet are the provision of digital information consisting of text, sounds, images, animations, music, videos, movies, games or a combination of parts and/or all of them, including in the form of streaming or download that uses Internet access services through telecommunication network providers.

Under these definitions, ecommerce, fintech, online games, social media, etc., will all be deemed to be OTTs and subject to the regulatory requirements. So too will various healthcare, education, logistics, and other service providers who utilise any type of electronic delivery option. Companies (OTTs) deemed not to be in compliance will have their bandwidth limited ("throttled"), and may be subject to fines or license withdrawal.

Raising taxation revenues from OTT service providers who do business in Indonesia, has become a major concern of the Ministry of Finance. The Tax Department in April 2017 issued a 'Circular Letter No. SE-04/PJ/2017 on the Determination of Permanent Establishments for Foreign Tax Subjects Which Are Providers of Applications and/or Content Services through the Internet ("Circular Letter 4/2017").' Under the circular, foreign OTT services that come within the meaning of permanent establishment[9] will be subject to Indonesian tax.

[8] Presidential Regulation No. 74 of 2017 on Roadmap for the National Electronic Commerce System for 2017-2019

[9] Permanent establishment within Indonesia includes: place for management activities; branch office; representative office; office buildings; garage or workshop; warehouse; physical space for promotional and sales activities; computers, including servers and data centers; electronic apparatus (i.e. devices which contain computer programs that may perform activities or which may respond based on automatic inputs); and other automatic devices. An OTT service provider is also to be considered as a

2.3 Good International Practices

Any regulatory framework should be technology-neutral to enable application of rules regardless of new technologies or changes in market and business models. The framework should be flexible enough to enable innovation and to ensure the application of benefits to society (e.g., improved education or healthcare) without having to frequently amend laws or implement new regulations.

- In Hong Kong, for example, when Voice over Internet Protocol (VoIP) was still a fixed line network service, VoIP service providers would only be allocated public call numbers if they provided an emergency call identification register, which needed to be updated whenever a customer relocated. Ultimately, the choice of provider (and therefore service) was left to the customer.

Policies should be formulated based upon clarity of services and markets; where traditionally regulated and non-regulated sectors are merging because of OTT services, the most beneficial approach appears to be one of light-touch regulation focused on the least competitive sectors.

- An example is the European Union (EU)'s "Better Regulation for Better Results Agenda" adopted in May 2015.[10] The approach explicitly recognises the unregulated and international nature of the Internet by applying a Regulatory Fitness and Performance Programme (REFIT) designed to regulate better by "removing red tape and lowering costs without compromising policy objectives". Policies are reviewed on a continuous basis to ensure that the regulations are "fit for fast-changing industries".

Policies should be based upon objective assessments of the social and economic impacts of various categories of OTT services; regulators should accumulate data from regulated markets for policy assessments, clearly articulating both the objectives and the data sources so as to avoid unintended consequences of poor policy and to maximize social welfare.

- In 2013, Singapore's then Media Development Authority (MDA) introduced regulation for OTT news websites to have a consistent regulatory framework for both traditional and online news sites. OTT news websites were required to be individually licensed if the following two criteria were met: "if they report an average of at least one article per week on Singapore's news and current affairs over a period of two months, and have at least 50,000 unique visitors from Singapore each month over a period of two months. The individual licenses have to be renewed every year."[11] In addition, a performance bond of SGD50,000 (USD37,000) was required.

permanent establishment if it provides any form of services for period of 60 days or more within any given 12-month period.

[10] European Commission, Better regulation for better results – an EU agenda (2015), p. 10 http://ec.europa.eu/smart-regulation/better_regulation/documents/com_2015_215_en.pdf

[11] Straits Times, MDA rolls out license scheme for news sites (May 2013), http://www.straitstimes.com/singapore/mda-rolls-out-licence-scheme-for-news-websites

3. Investment

3.1 Issue Overview

Investment into local SMEs and the local use of digital technologies encourages competition. Any unnecessary constraints on such investments will therefore threaten to undermine potential competition, innovation and opportunity.

Investment into Start-Ups

A start-up is a young company, just beginning to develop, and with the ability to grow a scalable business model. These companies offer a product or service that is not currently being offered elsewhere in the market, or is being offered in an inferior manner. Often start-ups adapt technology to solve these unmet needs.

Start-ups are usually small and initially financed and operated by a handful of founders or one individual. Typically, angel investors and venture capitalists fill financial gaps by providing initial funding in exchange for equity or some form of control over the business.

These areas and opportunities have been attracting particular interest as the digital economy (and the Internet economy before it) have grown. They have also been seen to have offered governments the opportunity to promote particular development priorities such as specific sectoral growth (e.g., biotech, Artificial Intelligence (AI), ecommerce, etc.), the promotion of micro-, small- and medium-sized enterprise (MSMEs), competitive disruption in certain areas, or as a means for attracting greater foreign direct investment (FDI) and intellectual capability.

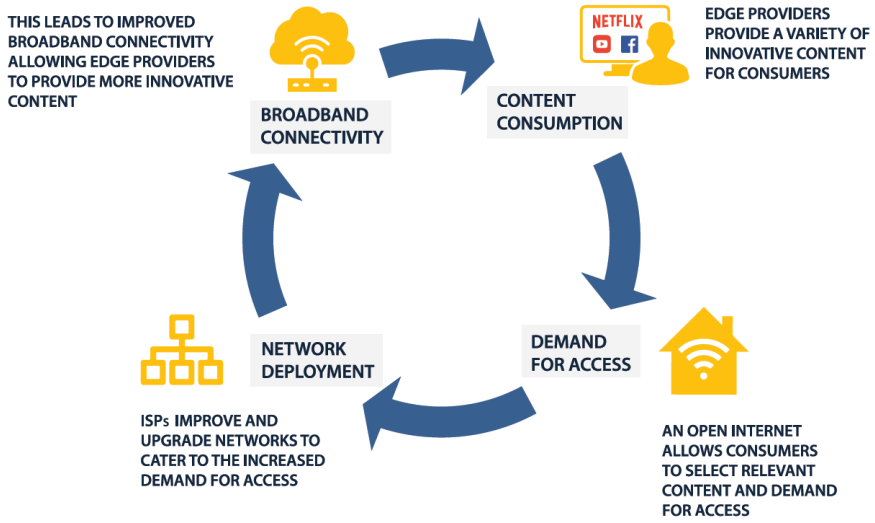
Investment into Infrastructure

One development that has become very apparent through the growth of the digital economy, the consumption of digital services (such as social media and video), and the accompanying explosion in data traffic required, is that the demand for content encourages more investment into the underlying Internet infrastructure, and this in turn improves Internet connectivity.

The result is a virtuous cycle of investment, consumption and demand (**Figure 1**) as consumers, increasingly able to access content at faster speeds and lower prices, increase their demand for digital services, which in turn spurs further investment into the infrastructure. This development has played out time and again globally – and, as noted above, challenges our conception of "an uneconomic consumer (or citizen)" and our models for calculating effective return on investment.[12]

[12] TRPC, *Connectivity, Innovation and Growth: Fostering an Open Internet in Asia* (January 2017), pp. 18-20 http://trpc.biz/connectivity-innovation-and-growth/

Figure 1: The Virtuous Cycle



The impact of OTTs therefore on competition and investment can be seen to be twofold:

- they reduce the market share and the *traditionally-collected* revenues (i.e., voice, messaging) of incumbent telecom providers and broadcasters, which could certainly have a negative impact upon investment in infrastructure from these players, by reducing their traditionally calculated rates of return on investment;[13] ***but***
- they add value by creating a *rapidly* growing consumer demand for last mile broadband capacity, and in many cases, they add value to the channels as bundled services of broadcasters.

The impact of OTT entry into telecom and broadcast markets is a positive one *in terms of investment*. That does not imply that traditional service providers are not financially challenged by their entry, but that their response needs to include new investment in extending local access to their networks, in upgrading the technology, and in making their core networks "super slim, cost efficient, and more agile".[14]

3.2 Investment in Indonesia

Indonesia's start-up ecosystem has enjoyed dramatic recent growth, due to the deeper penetration of the Internet, smartphones and social media. Over the past five years,

[13] In one scenario by McKinsey, by 2018 in terms of revenues, OTT players could account for 60% of messaging, 50% fixed voice calls and 25% mobile voice calls, up from 9%, 11% and 2% in recent years. McKinsey (January 2017) "Overwhelming OTT: Telcos' growth strategy in a digital world" http://www.mckinsey.com/industries/telecommunications/our-insights/overwhelming-ott-telcos-growth-strategy-in-a-digital-world

[14] McKinsey estimate between 30% and 70% network costs could be saved. McKinsey (January 2017) "Overwhelming OTT: Telcos' growth strategy in a digital world" http://www.mckinsey.com/industries/telecommunications/our-insights/overwhelming-ott-telcos-growth-strategy-in-a-digital-world

Indonesia's start-up investment has grown 68 times, reaching USD1.4 billion in 2016, and jumping to USD3 billion in the first eight months of 2017.[15]

A joint report by Google and AT Kearney, highlights four areas to accelerate the growth of the start-up ecosystem in Indonesia:[16]

- talent development;
- fiscal incentives;
- funding and exit options; and
- start-up facilitation.

In June 2016, the Gerakan Nasional 1000 Startup Digital initiative was launched. The government-backed program aims to grow 1000 start-ups by 2020.

3.3 Good International Practices

Investment into Start-Ups

A start-up ecosystem, including local SMEs, incubators and accelerators, and venture capital, is essential. SMEs need finance capital and professional experience and advice.

As evidenced in mature markets, governments can play a strong role in facilitating investment. The Singaporean government provides a host of start-up related grants and support schemes under StartUp SG. It nurtures start-ups through mentorship and networks; incubators and accelerators; early-stage funding; commercialising ideas; equity investment; and going to market. It provides access to local support initiatives including:

- a platform for matching mentors to start-ups, as well as funding up to SGD30,000 (USD22,000) to first-time entrepreneurs with innovative business ideas by matching SGD3 to every SGD1 raised by the entrepreneur for up to SGD30,000;
- fast-tracking the development of proprietary technology solutions;
- a scheme where the government co-invests with independent, qualified third-party investors in a start-up;
- incubators and accelerators in strategic growth sectors;
- facilitating a conducive environment for global talent to join local start-ups and set up innovative businesses in Singapore;
- government-backed loans for start-ups' working capital, equipment/factory financing and trade financing needs, offered through participating financial institutions.

Investment into Infrastructure

Indonesia, can appear in some contexts, to be one of the most highly connected economies in the region: often touted as the "no.4 Facebook community globally", and the "Twitter capital of the world," Indonesians often adopt new technology at a rapid rate. But not only is such

[15] Google and AT Kearney, Indonesia Venture Capital Outlook 2017 (September 2017), http://www.southeast-asia.atkearney.com/paper/-/asset_publisher/dVxv4Hz2h8bS/content/indonesia-venture-capital-outlook-2017

[16] Google and AT Kearney, Indonesia Venture Capital Outlook 2017 (September 2017), http://www.southeast-asia.atkearney.com/paper/-/asset_publisher/dVxv4Hz2h8bS/content/indonesia-venture-capital-outlook-2017

connectivity highly and disproportionately concentrated on urban or wealthier environments, the connectivity itself is disproportionately focused on social media and social connectivity – some 80-90% of digital activity – with far less usage directed towards economic, trade or social development activity. Thus, it hasn't been translated into accompanying economic value yet. This requires focusing on human capacity – digital literacy, and the facilitation to be able to use connectivity to have and to generate economic value – in parallel.

Such developments point to the issue of governance, on the one hand, and the realities of cross-border trade, on the other. There is a need to rethink both the approach and the coordination mechanisms required to drive a successful digital economy framework. As has been repeated in many different contexts, the Internet knows no borders. This is a strength in providing access to a global market, in lowering costs, and in accelerating and democratizing innovation. But increasingly the challenges too are becoming apparent: differences in the levels of market development when coupled with digital opportunity have rapidly challenged the ability of policy makers to effectively control policy and regulatory levers, in everything from cybersecurity to privacy, piracy and on to tax regimes and identity. The ability of domestic policymakers and regulators to stipulate and enforce decisions has been challenged and eroded. (This is further detailed below).

Networks are part of the Critical National Information Infrastructure (CNII), and as such regulations are required to ensure their availability at reasonable cost. This was a more straightforward regulatory task when networks were near-monopolies, but the results often left major gaps in geographical coverage, slow technological progress and little in the way of service innovation. This changed when effective competition was established, but regulations to ensure that competition was effective and appropriate changes in the way licensing and the assignment of radio spectrum took place, became a major challenge. The big advantage of growing domestic competition was that new sources of funding network development opened.

- In March 2017, the Philippines introduced the National Broadband Plan partly to spur investments into unserved and underserved areas in the country. Priority is given to areas with high density but low coverage. The Plan specifically calls for the greater use of public-private partnership arrangements so as to fund infrastructure such as fibre optic submarine cables, landing stations, cell sites, and shared infrastructure such as base stations.

The emergence of OTT services has further introduced another source of funding for international and long-distance networks and content distribution networks (CDNs).

- Facebook and Google, for example, have begun investing heavily in submarine optical fibre cables to guarantee fast and secure data traffic delivery, including the Pacific Light Cable Network with a designed capacity of 120Tbps, connecting the USA and Hong Kong directly from 2018 (the first of its kind). The capacity requirements of these OTT players are now exceeding those of the largest carriers.[17]

[17] TeleGeography reported in 2016 that private networks already account for around 50% of the intra-Asia and trans-Pacific traffic. TeleGeography, *Global Bandwidth Research Service: Executive Summary* (2016), https://www.telegeography.com/page_attachments/products/website/research-services/global-bandwidth-research-service/0006/7209/gb16-exec-sum.pdf

- Licensing reform can turn the challenge of OTT into an opportunity. A good example is India, the first country to introduce unified licensing in 2013, a recognition that convergence of fixed and mobile, voice, text and video, offered opportunities to attract new investment into the information and communications and media sector.[18]

The biggest challenge remains investment in local access networks, but high-speed mobile broadband networks are now starting to fill a major part of this gap.

4. Net Neutrality and Network Management

4.1 Issue Overview

A robust and reliable digital infrastructure with access to service providers and customers is a fundamental requirement of a successful digital economy. In addition to investment into the infrastructure, access and affordability are essential requirements, as are policies that promote inclusion.

As Indonesians have a higher-than-average usage of social media and digital entertainment consumption, it is important to ensure – as far as possible – equal access to all sorts of content by users. It is important therefore that there is an effective net neutrality framework by regulators, telecom operators and internet service providers (ISPs), so that users can freely choose to use and access all types of digital service providers. This includes non-discriminatory zero-rating schemes developed to promote innovation while enabling access in markets where affordability remains a challenge.

The central debate of net neutrality has been focused on whether network providers should be allowed to charge digital service providers for interconnecting with their networks — prioritizing certain traffic by creating “fast lanes” for their preferred content and services.[19] This may lead (inadvertently or otherwise) to digital service providers raising prices to afford the additional fees or reducing investments into developing content and services — constraining future innovation and the entrance of new players.

The lack of net neutrality can also reduce consumer ability to choose freely with choices instead being made for them by network intermediaries. Under net neutrality, the principle of non-discrimination informs the business models of both content and network providers benefitting consumers and creating a competitive environment for innovation.

The issue of net neutrality is sometimes confused with the wider issue of censorship. All countries within the Asia-Pacific region have laws allowing for the blocking of certain websites, *but not for commercial reasons*.

[18] TRAI, Unified Licensing Regime – Indian Case Study (2013), https://www.itu.int/ITU-T/worksem/conreg/presentations/conreg_0504_sapna_sharma.pdf
[19] Cyber Telecom, Internet Interconnection (2016), http://www.cybertelecom.org/broadband/backbone2.htm

Network Management

Efficient network management is essential in ensuring the smooth transit of traffic and the high-quality delivery of content to all users over the Internet. Networks face variation in usage patterns due to time differences, geography and user demographics.[20]

"Network management" is an increasingly broad term that encompasses a set of functions used by ISPs, digital service providers (including cloud computing providers) and telecom operators to deploy bandwidth at peak hours. This is done by conducting network planning, load balancing and utilising other tools available.

However, network management must not become a smokescreen for discriminatory and anti-competitive behavior. For example, managing specific digital service providers by throttling or filtering would not address the shortage in supply of Internet "lanes" during peak hours.

Net Neutrality

The principle of net neutrality is that ISPs should enable access to all content and applications regardless of the source, and without favouring or blocking particular products or websites.[21] For example, if an ISP charges more for higher than for lower bandwidths and speeds, access to applications and content will not be equal. However, if every customer has an equal opportunity to choose their access plan, then there is equality. If there is a digital divide with higher bandwidths and speeds available only in some regions and not others, access across regions is not equal, and this will become replicated in both the delivery and consumption of services – if the experience is unsatisfactory, people will turn away.

There remains a division of opinion as to whether it is equality if all digital services providers are faced with a choice to pay their ISP for a better quality of access, or to accept a lower standard of access at a lesser charge or no charge. One distinction in approaching this issue is whether the service being provided is a "passive" one, e.g., where a user accesses a website for the progressive download of a video, or an "active" one, in the sense of streaming video to a customer. Both could involve a payment, but the active commercial sites are more likely to be engaged in revenue generation, and to be more concerned with the quality of reception.

4.2 Net Neutrality and Network Management in Indonesia

OTTs

Kominfo's OTT draft regulation does not support the principle of net neutrality. Under the draft regulation, OTT service providers are obliged to store data on transactions and traffic for three months, guarantee legal access to that data for investigation purposes, and set up a customer inquiries and complaints information centre and respond to requests and complaints within 48 hours. OTT service providers may collaborate commercially with telecom companies, in which case they should provide the scope of collaboration; roles and responsibilities of each party; business scheme; tariff structure; etc. OTTs who violate the regulations will have "bandwidth

[20] *Sandvine*, Reasonable Network Management: Best Practices for Network Neutrality (2017), https://www.sandvine.com/downloads/general/whitepapers/reasonable-network-management.pdf
[21] Save the Internet, Net Neutrality: What You Need to Know Now (2017), https://www.savetheinternet.com/net-neutrality-what-you-need-know-now

management" – i.e., "bandwidth throttling" – imposed upon them and carried out by the telecom service provider.

National Payment Gateway

In 2016, Indonesia had 424 million ATM/debit transactions in the country.[22] Payment companies had a choice on the switching companies they partnered with to process transactions in Indonesia, and had the freedom to choose where these transactions were routed to.

In July 2017, Bank Indonesia (BI) released the NPG regulation. The regulation seeks to make transactions easier and cheaper for customers by allowing all electronic money, debit and credit cards of any issuers to be accepted at any ATM, electronic data capture device or payment gateway. However, all domestic transactions will be required to be processed through the NPG. The regulation also requires all parties connected to the NPG to be members of at least two switching agencies.

The NPG in its current form poses challenges for ecommerce transactions, given that ecommerce transactions utilise credit cards. It also raises transactional issues across several sectors and has left it unclear whether international transactions are also required to be processed through the NPG. Network management, security and access issues are all further important considerations.

4.3 Good International Practices

Network Management

Regulators have little direct access to the management of networks, so a set of metrics to help monitor and evaluate network management is useful. For example, the following guidelines should raise potential red flags for regulators:[23]

- management techniques applied in or below the transport layer affecting transit between networks;
- tools involving termination or blocking as opposed to traffic shaping and queueing;
- if the request is a unilateral decision from the service provider rather than coming from the user end or the source end; and
- when a network management tool is applied to (i) apps, (ii) the source/destination, (iii) the service provider, or (iv) the payments processor.

Internet Exchange Points (IXPs) bring content closer to consumers, lower network costs and decrease latency, which ultimately makes the distribution of content more efficient. These practices are particularly important given that 56% of Asian Internet traffic originates from international sources.[24] The use of neutral IXPs negates the "tromboning" of data traffic,

[22] Bank Indonesia, ATM/Debit Card Transactions (2017), http://www.bi.go.id/en/statistik/sistem-pembayaran/apmk/Documents/Transaksi%20Kartu%20Debet%20Tahun%20(en).pdf
[23] Scott Jordan and Arijit Gjosh, How to determine whether a traffic management practice is reasonable (2009), http://www.ics.uci.edu/~sjordan/papers/tprc09.pdf
[24] TeleGeography, Global Internet Geography (2016), https://www.telegeography.com/products/global-internet-geography/analysis/regional-analysis/asia/index.html

wherein traffic is sent from a source point via a distant third country, often the US or Europe, before returning to the point of destination in the same country as the source.

According to the World Bank, "as the digital economy grows, so will the number and type of parties connecting to IXPs. For example, in Europe between 2008 and 2010 the percentage of connections to IXPs from content providers increased from 85% to 96.3%, by VoIP providers from 36.8% to 48.1%, by enterprises such as airlines and banks from 30% to 46.2%, by search engines from 25% to 48% and by governments from 50% to 77.8%. For developing countries, these are trends to take note of as *IXPs have an important role in triggering and accelerating the local digital economy*, so even if an IXP initially requires some form of subsidy, if successful it will generate sufficient volume of traffic and make itself sustainable."[25] At that point, different charging models can be adapted to suit local circumstances. This virtuous cycle whereby a carrier-neutral IXP attracts content caching, making it increasingly available and stimulating further usage has been replicated in many markets. For example, in Kenya IXP traffic rose tenfold in one year following the installation of Google Global Cache.[26] An exception would be in territories where Internet traffic is already monopolised by the incumbent.

The Internet Society developed an IXP Toolkit to provide guidance on best practices to implement IXPs.[27] The Toolkit contains case studies on how different countries set up, run and manage IXPs. Biznet Indonesia eXchange (BIX)[28] was used as an example for Indonesia, connecting local points-of-presence (POPs) to the Internet. It has multilateral peering agreements on exchanging Internet traffic, keeping traffic local and increasing the efficiency of content distribution.

Singapore, Hong Kong, and Tokyo are established international Internet hubs for exchanging traffic and hosting content which enjoy lower transit costs than recently developed markets such as Jakarta and Bangkok. The 2016 median monthly IP transit price per Mbps was USD9 in Jakarta, USD10 in Bangkok, while only USD3.15 in Hong Kong and Singapore, and USD3 in Tokyo.[29] By encouraging international and local ISPs, cloud and content providers, and Internet service providers to interconnect and freely exchange traffic, they create more direct routes which are increasingly important for bandwidth-heavy content such as video streaming and online games.

The Singapore Internet Exchange (SGIX) has three points-of-presence in the country, and boasts 92 peering members, including all local ISPs, domestic and international telecom carriers and major cloud and content providers such as Netflix, Google, Microsoft, Cloudfare

[25] World Bank (2013), *IP-Based Interconnection, Broadband Toolkit,* ch 3.4, http://broadbandtoolkit.org/3.4; data from S, Silvius (2011), *Internet Exchange Points* https://www.euro-ix.net/documents/894-ixp-research-pdf?download=yes
[26] infoDev (2011), *Broadband in Kenya: Build It and They Will Come*, http://broadbandtoolkit.org/Custom/Core/Documents/ke.pdf
[27] IXP Toolkit (n.d.), https://ixptoolkit.org/
[28] IXP Toolkit, Indonesia (n.d.), https://ixpwp.isocdev.org/indonesia/
[29] Telegeography (2016) Median Monthly 10 GigE IP Transit Prices in Selected Cities, 2013-2016, https://www.telegeography.com/products/global-internet-geography/capacity-and-pricing-data/summary-data-and-charts/index.html

and others.[30] When SGIX first began in 2009, it had 11 members. As an open, neutral, and not-for-profit IXP, SGIX has managed to attract a large membership of domestic and international providers by employing an open system where providers are not discriminated against, are charged low costs for peering, and have low requirements for participating. In Singapore, the then Infocomm Development Authority (IDA) proposed the establishment of the Singapore Internet Exchange (SGIX) in 2009 to strengthen Singapore's position as an "infocomm hub", lowering interconnectivity costs for local and international ISPs, improving network resiliency, and providing an enhanced online experience for consumers.[31]

Net Neutrality

The principles of net neutrality are widely supported, and the debate is, to a large extent, more about how far can market forces be expected to ensure a desirable outcome rather than, or with minimal, regulation.

Within the Asia-Pacific region, some OTT providers have already collaborated with local ISPs, enhancing the value of the ISP network in the process, and competition, especially from the rapid growth of broadband mobile networks and the spread of smartphones and other smart devices.

- In 2010, Chile became the first country in the world to enact legislation safeguarding the principles of net neutrality and establishing transparency obligations for ISPs. It has allowed entry of new operators into the market, thereby increasing competition and lowering costs. According to SUBTEL, a local telecoms authority in Chile, between 2009 and 2012, the number of mobile connections increased from 600,000 to nearly five million, while fixed connections increased from 1.7 to 2.2 million. In 2012, the costs to users also decreased up to 50% in the price of services.[32]
- In 2011, Singapore's regulator issued guidelines supporting net neutrality rules.[33] ISPs are allowed to sell "fast lanes" for a fee as long as they continue to provide good service levels to average users. However, ISPs are not allowed to block legitimate Internet content, or degrade access to websites, apps or services to the point that they become unusable.
- In 2012, the Netherlands was the first EU nation to pass legislation on net neutrality. This legislation was revised in 2016 to ensure that telecom operators and ISPs treat all internet traffic equally and cannot favour one Internet app or service over another.

[30] SGIX (2016) Peering Members, http://www.sgix.sg/peering-members/, accessed 7 Dec 2016

[31] IDA, Singapore Internet Exchange Fact Sheet (2013), https://www.imda.gov.sg/~/media/imda/files/industry%20development/infrastructure/sgix_factsheet.pdf?la=en

[32] Digital Rights – Latin American & The Caribbean, An evaluation of the net neutrality law in Chile (July 2013), https://www.digitalrightslac.net/en/una-evaluacion-de-la-ley-de-neutralidad-de-la-red-en-chile/

[33] IDA, Decision issued by the IDA of Singapore: Net Neutrality' Singapore (June 2011), https://www.imda.gov.sg/~/media/imda/files/inner/pcdg/consultations/20101111_neteutrality/netneutralityexplanatorymemo.pdf

5. Consumer Protection and Competition

5.1 Issue Overview

Governments should promote competition and fair trade in markets to benefit consumers, businesses, and the community. This involves regulating against anti-competitive behaviour to protect consumer rights as genuine competition is a driver of innovation and customer service. Consumer protection has long been a central feature of telecoms regulation, covering areas such as accessibility, pricing, quality of service, unfair and obscure contracts with tie-in clauses and other anti-competitive practices, undue sales pressure, transparency in billing, emergency call numbers, dispute resolution, etc.

In the digital economy, governments and competition authorities must address the challenges of protecting and empowering consumers in a complex and rapidly developing online environment.

Ecommerce has brought many benefits to consumers, including wider choices at competitive prices, as well as easy-to-use and more secure payment options. However, the higher complexity of the online environment also creates risks for consumers. A growing number of online platforms, such as social media platforms, offer "free" services in exchange for consumer data. While the data use can be beneficial to both businesses and consumers, the risk environment is higher and offering these services could trigger consumer protection responsibilities.[34]

As discussed in detail above (see Section 2), technology has the potential to dramatically increase competition. However, digital service providers are also proving to be adept at accruing market share. In contrast to previous eras of development, this accrual of market share is often the first step in a digital service provider's business strategy – and may be their only strategy (particularly if they intend to be bought out by a bigger company). Further complicating the issue, as we have seen, is that the market share of a digital service provider can extend across multiple verticals, and they may well utilize a dominant platform in one sector to leverage market share in another sector.

A prominent argument from telecom providers and broadcasters is that OTT service providers do not pay license fees and are not subject to similar regulations governing their operations or their content. The complaint is that there is an "uneven playing field". The real issue is whether the barriers to entry prevent competition, and whether they are "natural" or induced, for example, by anti-competitive practices or by exclusive licenses.

Online platforms have direct and indirect network effects with tendencies towards natural monopolies. The higher usage of types of digital services (such as social networking sites, and voice and messaging apps) leads to more efficient service delivery and results in the dominance of only a few digital service providers. However, *dominance is not necessarily a*

[34] OECD, Consumer Protection in E-Commerce: OECD Recommendation (2016), pp. 4-5, http://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf)

problem in itself. Dominance only becomes an issue when digital service providers abuse their dominance to the detriment of consumers or engage in unfair conduct.[35]

Applying existing regulatory frameworks and models in the digital space requires judgement. The changing landscape needs to be taken into account. A recent editorial in the *Financial Times* made three astute points in this regard:[36]

- Competition authorities should shift focus from the definition of markets to the realities of customer lock-in.
- The interoperability of networks – which interconnect through the Internet – carrying OTT apps and content will become increasingly an important focus, especially with the spread of the Internet-of-Things and sensor-directed edge networking.
- The growing use of algorithmic pricing for digital services, such as taxi-hailing apps, erodes consumer surplus – the difference between higher prices consumers are willing to pay and lower prices they are required to pay. The analytical challenge posed by competition is that, like collusion, it produces similar prices for similar products and services in the marketplace. Digitalised OTT services and the use of algorithms make these distinctions more difficult for regulators to judge.

5.2 Competition and Consumer Protection in Indonesia

Currently overlapping regulatory mandates hinder consumer protection for users in Indonesia. Recently proposed draft regulations, such as Kominfo's draft OTT regulation and the Transport Ministry's ride-hailing regulation for example, provide separate – and at times contradictory – adherence levels for digital service providers.

In July 2017, the Transport Ministry's ride hailing regulation (no.26/2017) came into effect, setting quotas for the number of cars in a city, and minimum and maximum tariffs for car-hailing services.[37] By doing so, the regulation limited the flexibility ride-hailing companies had in setting prices driven by customer supply and demand and altered the competition between online platforms, such as Go-Jek and Blue Bird.

One month after the regulation came into effect, in August 2017, Indonesia's Supreme Court ruled that the regulation on tariff setting was illegal *as it impeded competition*.[38] The Transport Ministry's revised regulation (no.108/2017), came into force on 1 November 2017, and does not contain major changes as base fares and caps will still be fixed, and fleet quota limitations will be imposed.[39] Under the revised regulation ride-hailing transportation services are

[35] European Commission, Abuse of dominant position (April 2012), http://ec.europa.eu/competition/antitrust/art82/
[36] Financial Times, Competition authorities need a digital upgrade (July 2017), https://www.ft.com/content/f6fe0f18-73d1-11e7-aca6-c6bd07df1a3c
[37] The tariffs are:
- Zone 1, comprising Java, Sumatra and Bali: IDR3,500-6,000 (USD0.26-0.49) per km
- Zone 2, comprising Kalimantan, Sulawesi, Nusa Tenggara, Maluku, Papua: IDR3,700-6,500 per km

[38] Reuters, Indonesia court scraps new ride-hailing tariff rules (August 2017), https://www.reuters.com/article/indonesia-transportation-ruling/indonesia-court-scraps-new-ride-hailing-tariff-rules-idUSL4N1L74HR
[39] Permenhub No 108/2017: https://kominfo.go.id/content/detail/11232/ini-9-aturan-baru-untuk-angkutan-online-versi-kemenhub/0/sorotan_media

required to operate in specific areas, are prohibited from picking up passengers directly on the street, are required to use mobile app technology and must have a minimum standard of service. Other stipulations include a requirement for vehicles to display stickers issued by the Transportation Ministry and to pass roadworthiness tests.[40]

The emerging new regulations also indicate a perception that consumers are not adequately protected unless rules and regulations are clearly defined in legislation. Such a perception, while understandable, has not been broadly borne out to date, and risks curtailing innovation and consumer welfare benefits before they can emerge. For example, *Article 8* of the draft regulation requires OTT service providers to set up a customer inquiries and complaints information center and respond to requests and complaints within 48 hours. Adopting a light-touch and *flexible* initial regulatory approach would be beneficial in providing quality choices to consumers and promoting innovation in the industry.

5.3 Good International Practices

Regulators need to be able to clearly determine whether a digital service (such as an OTT service) warrants a degree of regulatory oversight or intervention before proceeding. For example, services that have major social impact are more likely to warrant a regulatory approach than others, although popular support for such measures can differ. Censorship of artistic content, for example, may receive only partial popular support, while blocking sites that espouse hate or abuse will be more acceptable to a wider audience.

If the consumer has choice, then the only regulations required are likely to be those that restrict choice. For example, in some countries, online gambling is prohibited, as is using websites to launder money or to buy prohibited items such as illegal drugs. Otherwise, issues such as price, terms and conditions of sale, etc., mostly can be left up to consumers to choose. From a policy and regulatory point of view, intervention may be justified where it is important to empower the consumer with information about the safety of websites, and how to secure their own personal data.

There are few markets more open to global competition than OTT markets, so from a consumer safeguard point of view, awareness is the key issue. For example, the consumer should check the availability of dispute resolution and refunds. These issues will normally come under the regulatory authority of fair trade bodies and consumer advisory councils, but if sanctions, such as fines or license suspensions, are involved, the telecom and broadcasting regulators have a role to play. Regulators should monitor digital service providers' compliance through regular reporting requirements on consumer complaints and their resolution.

Besides OTT services that stream content and apps to consumers, there are websites, such as ecommerce sites and gaming sites, which require constant pro-active consumer behaviour. Some of these sites, such as social media sites, have significant social traction, and the regulation of content will always be an issue. This is more complicated when the traffic is encrypted end-to-end, as it is increasingly so on texting sites, but could equally be applied to audio-visual sites. Collaboration between telecom and broadcast regulators and cybersecurity agencies and the police will become more frequent and institutionalised. But in other cases,

[40] Jakarta Post, New ride-hailing transport regulation in place (October 2017), http://www.thejakartapost.com/news/2017/10/30/new-ride-hailing-transport-regulation-in-place.html

such as sites offering online commerce services, the role of regulation will be limited to three areas, and only the third will involve telecom and broadcast regulators directly. They are:

1. the sale and purchase of prohibited items;
2. the payment of custom and excise duties, if applicable; and
3. any violation of net neutrality rules, where these may apply.

Best practices in promoting competition seek to ensure there are no unnecessary restrictions that may hinder innovation.

- In June 2017, the EU introduced a new rule on the use of digital services. EU residents who paid for the services in their home country will be allowed to access the service while visiting another country within the EU.[41] EU residents will be able to access content such as music, e-books, videos without extra cost for services paid in their home country. This new rule is able to increase competitiveness among digital services and encourages providers to ensure the same level of accessibility in all EU countries. Without these "roaming rates", it encourages more consumers to subscribe to digital services.
- Singapore is working to introduce a new standard on the interoperability for IoT devices. In September 2017, the government announced that it will conduct a trial to test whether a new standard for Over-The-Air Subscription Management (OTASM) can "enable SIM chips embedded in IoT devices to switch between different network operators".[42] Currently, each SIM is tied to a mobile network and interoperability has not been enabled. The introduction of the standard will encourage the development of IoT products and software, enabling the devices to "talk" to each other, while reducing costs for businesses.
- Bahrain's Telecommunications Regulatory Authority (TRA), in recognising that OTT service providers compete against traditional telco companies, recommended to continue to allow for competition of OTT service providers, as "instituting a ban will limit innovation and hinder competition. Businesses will evolve to adapt to consumer preferences, and will be challenged by new businesses that introduce innovation and hence competitive pressures in the market."[43]

Regulatory Sandboxes

In terms of promoting cross-sectoral competition and being able to assess the need for employing new regulatory regimes, one tool that governments are looking to employ are regulatory sandboxes that enable experimentation and innovation to foster the growth of the digital economy. A regulatory sandbox that is open to businesses of any size can serve as an accelerator for technological innovation.

[41] European Council, Portability of digital services across the EU: Council adopts new rules (June 2017), http://www.consilium.europa.eu/en/press/press-releases/2017/06/08/portability-of-digital-services/

[42] Infocomm and Media Development Authority, Leading the Charge for Open IoT Standards (September 2017), https://www.imda.gov.sg/infocomm-and-media-news/whats-trending/2016/1/leading-the-charge-for-open-iot-standards

[43] Detecon Consulting, Policy and Regulatory Framework for Governing Internet Applications (March 2014), http://www.tra.org.bh/media/document/Study_Policy_Regulatory_Framework.pdf

The sandbox approach enables government and the private sector to work together to develop innovations, whilst maintaining regulatory oversight and ensuring consumer protection. Further, it improves the capacity of regulators by enabling real-time practical experience in working with the private sector on new tech-driven development and innovation.

A regulatory sandbox should:

- be intended to encourage experimentation using the most current and innovative technologies;
- provide the opportunity for companies to have a dialogue with the regulator and demonstrate their assessment of the innovation without any judgement or preconceptions; and
- provide guidance, particularly for new entrants, perhaps not yet licensed, on how to develop and comply with legal and regulatory requirements.

A regulator may institute a regulatory sandbox to advance industry through innovations that provide newer services, improve current business operations or provide better services to individuals. From the regulator's perspective, the regulatory sandbox is designed to address the concern that regulations may be a barrier to innovation, and enables the regulator to be more responsive and to respond in a far nimbler fashion to technology disruption.

A business would seek to bring a project to the regulatory sandbox, when the proposed project would either not fit within or be unduly restricted by current law or regulations; or both the regulator and the applicant may be unclear how the existing regulatory framework would or should apply to the proposed solution. The regulatory sandbox enables the company and regulator together to develop insights into applicability or potential regulatory changes that may need to be made when taking the project into a live environment with regulated workloads.

Regulatory sandboxes, to date, have been largely focused on the financial sector, but in reality can be utilised by any sector (e.g. transportation, education, health), as they provide a solid framework for enabling cross-sectoral participation and innovation. Fintech regulatory sandboxes are now increasingly being established by financial regulators around the world, including in Hong Kong, Australia, Singapore and Malaysia.

The Monetary Authority of Singapore (MAS) launched a FinTech Regulatory Sandbox which aims to transform Singapore's financial sector by: increasing efficiency; improving risk management; creating new opportunities; and improving people's lives.[44] MAS is encouraging innovation and experimentation by start-ups and established financial institutions to ensure that promising innovations can be tested in the market and have a chance for wider adoption, in Singapore and abroad. This also limits an over-abundance of caution by start-ups and established financial institutions when launching new products.

PolicyPal (www.policypal.com), a Singapore-based insurance-tech start-up, became the first start-up to graduate in August 2017, having entered the six-month MAS sandbox in March 2017. The MAS Sandbox enabled PolicyPal to experiment with technology applications and

[44] Monetary Authority of Singapore, Fintech Regulatory Sandbox Guidelines (November 2016), pp. 4-5 http://www.mas.gov.sg/~/media/Smart%20Financial%20Centre/Sandbox/FinTech%20Regulatory%20Sandbox%20Guidelines.pdf

different product offerings under a well-defined space and duration. PolicyPal has now commenced operations as a registered direct insurance broker. It provides consumers with an alternative platform that utilizes artificial intelligence to simplify and digitise insurance.[45]

Bank Negara Malaysia (BNM) launched a Financial Technology Regulatory Sandbox Framework which aims to support innovations that will improve the quality, efficiency and accessibility of financial services in Malaysia. To modernize the financial sector, the sandbox reduces the regulatory constraints in launching innovative products or services. BNM reviewed the initial standards to encourage the wider participation of fintech companies. Currently, applicants can include a financial institution; a fintech company that collaborates with a financial institution; or a fintech company that intends to carry on an authorized or registered business.[46]

Malaysian owned start-ups, **MoneyMatch** (https://moneymatch.co) and **GetCover** (http://getcover.asia), are two of the four approved participants currently experimenting in the BNM sandbox. MoneyMatch is developing its own platform to provide cross-border remittances and money changing services by matching individual buyers and sellers of currencies. This caters towards the SME market in Malaysia, which currently completes a number of cross-border transfers in the normal course of business. GetCover, an insurance aggregator, intends to offer an app that allows consumers to buy motor insurance directly from insurers. This benefits consumers by consolidating market research within the app, and streamlines operations and decreases distribution costs for providers.[47]

6. Data Protection and Security

6.1 Issue Overview

Data protection falls into two broad categories: protection of personal data privacy, and protection of data of any kind from cyber-attack or from transfer to unauthorized parties at home or abroad. Data protection, including security, confidentiality, and preserving the integrity of data, is a core data management responsibility. A component of data protection is the protection of an individual's personal data, or privacy protection.

Technology has transformed almost all aspects of social life (in addition to the economy), facilitated and driven by the free flow of data, *including personal data*. The benefits from *cross-border* data flows include market access through trading opportunities, investment, innovation, development and growth, and an increase in productivity. This trend will only grow as the processing and analysis of large amounts of personal data become possible with increasingly sophisticated technology. However, there are growing concerns from individuals about how their data is being collected, used and transferred to third party organizations.

[45] *Straits Times*, "Insurance start-up PolicyPal graduates from MAS fintech regulatory sandbox" (August 2017), http://www.straitstimes.com/business/companies-markets/insurance-start-up-policypal-graduates-from-mas-fintech-regulatory
[46] Bank Negara Malaysia, Financial Technology Regulatory Sandbox Framework (October 2016), http://www.bnm.gov.my/index.php?ch=57&pg=137&ac=533&bb=file
[47] *The Star*, "Bank Negara kicks off fintech sandbox" (May 2017), https://www.thestar.com.my/business/business-news/2017/05/29/bank-negara-kicks-off-fintech-with-licences-issued/

Addressing these developments requires a coherent data protection framework to underpin the digital economy and enhance trust. Any data protection framework will need to be flexible to further enable innovation.

Compounding this challenge is the ever-increasing threat of cybersecurity. As economies "go digital", the risk of cyber-attacks becomes universal. Although the responsibility of cybersecurity rests primarily with the organizations or enterprises involved, there are two outstanding areas in which regulators have a leading role to play. First, protection of the critical national infrastructure. Second, enforcement of regulations that require organizations that have suffered an attack, and possibly lost customer information, to pass that information onto regulators and users as soon as practical.

Indonesia, like most other jurisdictions, needs to construct a data governance framework that takes into account these considerations.

6.2 Data Protection and Security in Indonesia

In December 2016, Kominfo issued Ministerial Regulation No. 20 of 2016 on Protection of Personal Data in Electronic Systems (data protection regulation).[48] This implements one of the provisions of Government Regulation No. 82 of 2012 (GR82)[49] under the umbrella of the Electronic Information and Transactions Law.[50] The data protection regulation provides a two year transition period for organizations to be fully compliant. The new data protection regulation covers the classification of personal data; protection of personal data; rights of personal data owners; and obligations of electronic system organizers.

The regulation adopts a very broad definition of personal data, which essentially could cover any information of an individual. It defines personal data as certain individual data which is stored, maintained and kept accurate and the confidentiality of which is protected. "Certain individual data" is defined as true and actual information that is attached to and identifiable towards, directly or indirectly, an individual. The regulation further defines electronic system organizers as every person, state official, business entity and or society who provides, manages and/or operates an electronic system individually or jointly to use for their purposes or the purposes of another party.

The rights of data owners mentioned in the regulation include the right of privacy of their data; the right to file a complaint over the failure of data protection by the electronic system organizer to the Kominfo Minister; the right to get access to modify, update or check the history of their data; and the right to ask for the destruction of their personal data.

Electronic system organizers have several responsibilities, including:

- certifying their system and maintaining confidentiality of personal data;

[48] Minister of Communications & Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in an Electronic System

[49] Government Regulation No. 82 of 2012 regarding Provisions of Electronic Systems and Transactions (GR82). The data protection regulation provides more detailed provisions than GR82 on how to use personal data in electronic systems in every stage of the process, including: acquisition, collection, processing, analysis, storage, display, announcement, transmission, dissemination and destruction of any personal data.

[50] Law No. 11 of 2008 regarding Electronic Information and Transactions (EIT Law) as amended by Law No. 19 of 2016 regarding the Amendment of EIT Law (EIT Law Amendment)

- notifying data owners over failure of data protection/breach; and
- having internal regulations managing the protection of personal data.

The element of express consent is highlighted throughout the provisions of data protection regulation. Any use of personal data by an electronic system provider, no matter how trivial, must be based on the consent of the personal data owner for that specific action. The consent must be in writing, whether manually or electronically, and in the Indonesian language (dual language formats are not prohibited). Further, the consent is only effective after a complete explanation from the electronic system operators on the intended use of the personal data.

The regulation of this prescriptive concept of consent in the digital economy, and the development of market practices remains to be seen.

The new data protection regulation does not reference definitions of "data controller" and "data processor" or distinguish between the roles. This imposes the same requirements on each, even though each has different responsibilities with regard to the data. These terms should be clearly defined in accordance with international standards and referenced consistently in all relevant laws and regulations. The adoption of the widely accepted paradigm of data-controller and data-processor will enable more uniform applicability of requirements and more consistent protection of data.

6.3 Good International Practices

Data protection and privacy law should be flexible to enable innovation. Legislation should be technology-neutral to enable applications of data protection and privacy rules regardless of the technologies involved. Overly prescriptive regulations could stifle the growth of the digital economy by creating undue economic burden or by serving as an inflexible barrier to innovation.

- The regulatory framework for data protection and data privacy should be risk based, rather than prescriptive. An example of a well thought out risk-based approach to data protection can be found in the APEC Privacy Framework, which recommends adherence to a set of privacy principles: Preventing Harm, Notice, Collection Limitations, Uses of Personal Information, Choice, Integrity of Personal Information, Security Safeguards, Access and Correction and Accountability.[51]

Countries across the Asia Pacific have implemented the APEC guidelines and have laws in place to protect personal data privacy, usually under the aegis of a Privacy Commission. In June 2017, South Korea was officially approved to join the APEC Cross-Border Privacy Rules (CBPR) system. It is the fifth country to participate in the system, joining the United States, Canada, Japan, and Mexico.

- New Zealand's Information Privacy Principles (IPPs) lay out the main requirements for handling personal information, forming part of the Privacy Act. The IPPs impose requirements for collecting, managing, using, disclosing and otherwise handling personal information collected from individuals. New Zealand's Privacy Act permits collection of personal data with notification and does not specifically require that

[51] APEC Privacy Framework, APEC Information Privacy Principles, Part iii (2005), http://publications.apec.org/publication-detail.php?pub_id=390

consent be obtained from the individual. The individual must be notified of the purpose for which the information is being collected and the consequences for the individual if the information is not provided.[52] The Privacy Act also recognises a distinction between principals and agents.

- Australia's Privacy Act (1988) includes thirteen Australian Privacy Principles (APPs). The APPs set out standards, rights and obligations for the handling, holding, use, accessing and correction of personal information (including sensitive information). The Privacy Act is primarily a notification based regime, and consent is required in limited circumstances.[53]
- Singapore's Personal Data Protection Act 2012 (PDPA) governs the collection, use and disclosure of personal data. It recognises both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes. The PDPA makes a distinction between an organisation that processes or controls/authorises the processing of personal data and a "data intermediary" who processes personal data on behalf of another organisation.[54]

Key Data Protection Principles

Governments should refer to international standards for requirements and procedures for the physical security of personal data and data privacy protection. Leveraging standards and industry best practices regarding security, privacy, and auditing provides assurance that effective physical and logical security controls are in place, and prevents overly burdensome or redundant processes.

There are many security frameworks, best practices, audit standards, and standardized controls that can be referenced, including:

- Service Organization Controls (SOC) 1/Statement on Standards for Attestation Engagements (SSAE) 16/International Standard on Assurance Engagements (ISAE) 3402 (formerly Statement on Auditing Standards [SAS] No. 70). Also SOC 2 and SOC 3;
- International Organization for Standardization (ISO) standards 27001; 9001; 27017; 27018;
- Federal Information Security Management Act (FISMA);
- Payment Card Industry Data Security Standard (PCI DSS);
- International Traffic in Arms Regulations (ITAR); and
- Federal Information Processing Standard (FIPS) 140-2.

A risk-based approach to security, and the adoption of industry best practices and international security standards such as the existing international standards for certification allow for flexibility and agility in adjusting to technology advances. Data governance is most agile and best conducted through self-regulation based on standards and best practices.

- In Australia, the Privacy Amendment (Notifiable Data Breaches) Act 2017 requires organisations to notify individuals as soon as practicable when there are sufficient

[52] Privacy Act 1993 (New Zealand), Principles 2 and 3
[53] Privacy Act 1988 (Australia), Schedule 1, Part 2
[54] Personal Data Protection Act 2012 (Singapore)

grounds to believe that the data breach is likely to result in serious harm to the individual.[55]

Data protection and privacy laws should be based on businesses adhering to the following key data protection principles:[56]

- **Fairness:** data subjects should be given accurate and full information about the data controller, purposes of processing, and any other information necessary to guarantee fair processing.
- **Lawful basis:** when deciding whether and for what purpose it will process personal data, the data controller must have a lawful basis for its processing.
- **Purpose limitation:** personal data may only be collected for specified, explicit and legitimate purposes, and not further processed in way incompatible with those purposes.
- **Rights of data subjects:** data subjects must be able to access their personal data, and obtain the rectification, erasure or blocking of personal data.
- **Accuracy:** data controllers must ensure personal data is accurate and kept up to date
- **Data security:** data controllers must implement appropriate measures to protect personal data from accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access.
- **Data retention:** personal data should not be kept for longer than is necessary for the purposes for which it was collected or processed.
- **Transfer**: personal data should not be transferred to a country or territory unless the country or territory ensures an adequate level of protection.

7. Data Localization

7.1 Issue Overview

The free flow of data, including personal data, has transformed both the economy and day-to-day lives of individuals. Benefits of cross-border data flows include market access through trading opportunities, investment, innovation, development and growth, and an increase in productivity. These benefits are best realized when there are no data residency restrictions.

In 2014, the free flow of data contributed USD2.8 trillion to the global economy,[57] a figure that could reach USD11 trillion by 2025.[58] Over the past decade, data flows are estimated to have increased world GDP by 10.1%.[59] With regard to cloud computing, security, business

[55] Privacy Amendment (Notifiable Data Breaches) Act 2017 (Australia)
[56] AWS EU Data Protection Whitepaper (Dec 2016), pp. 11-16, https://d0.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper_EN.pdf
[57]McKinsey & Company, Digital globalization: The new era of global flows (February 2016), http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.
[58] McKinsey & Company, By 2025, Internet of things applications could have $11 trillion impact (July 2015), http://www.mckinsey.com/mgi/overview/in-the-news/by-2025-internet-of-things-applications-could-have-11-trillion-impact
[59] McKinsey & Company, Digital globalization: The new era of global flows (February 2016), http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.

continuity and resilience are enhanced by the ability to manage data in geographically disparate locations.

What is important to understand is that facilitating cross-border flow of data does not need to undermine a government's ability to protect privacy, ensure regulatory oversight and compliance, or ensure national security. While often well-intentioned, cross-border transfer restrictions and data localization measures may not address the primary concern of data security. Security is not enhanced simply because data resides within a particular jurisdiction. Rather, security is a function of the technical know-how and financial capacity of a company to protect data.

Restrictions on data transfers are separate from restrictions on the collection of data. The latter either require consent by the data owner, or the data is independently and legally collected and/or mined from social media and other public sites. But if that data is deemed "sensitive", such as personal health data, certain financial records, or data deemed to be of national security, restrictions can apply. In some cases, however, countries have begun to assert "data sovereignty" demanding that *all data*, and especially data considered nationally strategic, *collected in-country must be stored in-country* (or at least replicated in-country and available for inspection).[60] Different agencies, such as the Privacy Commissioner, the central bank or monetary authority, or the police may be involved – further complicating clarity around the issue.

7.2 Data Residency Requirements in Indonesia

In Indonesia, GR82[61] (under the umbrella of the Electronic Information and Transactions Law[62]) and related regulations limit the ability of organizations to take advantage of technologies, such as cloud computing, that require cross-border data flow.

Article 17 (2) of GR82 and draft regulations on ecommerce and OTT services, require data centers that have information on public services, and disaster recovery centers to be located in Indonesia.

Amendments to GR82 are said to classify data into different categories but this has yet to be confirmed or implemented.

Indonesia also has sector specific rules that are relevant to data localization. For example, OJK issued POJK38/2016, where banks are required to use disaster recovery plans in Indonesia. There are exceptions to the rule, where banks can host specific information outside of Indonesia, with OJK's approval, provided that the data does not contain identifiable customer information.

[60] A useful summary of restrictions on data transfers and data sovereignty issues is ACCA/APCC (2014) *Report on Cloud Data Regulations: A contribution on how to reduce costs of Cross-Border Data Transfers* http://trpc.biz/wp-content/uploads/APCC-ACCA_WhitePaper_CloudRegulations_2014_FullPaper.pdf

[61] Government Regulation No. 82 of 2012 regarding Provisions of Electronic Systems and Transactions (GR82).

[62] Law No. 11 of 2008 regarding Electronic Information and Transactions (EIT Law) as amended by Law No. 19 of 2016 regarding the Amendment of EIT Law (EIT Law Amendment)

7.3 Impact of Data Localization

A 2014 ECIPE study estimated the economic costs related to proposed or enacted data localization requirements and related data-privacy and security laws in various countries including Indonesia.[63] The impact of proposed or enacted data restrictions on GDP was shown to be substantial in all seven countries, and in Indonesia was estimated to reduce GDP by 0.5%. If applied across all sectors, it was estimated to reduce GDP in Indonesia by 0.7%.[64]

An economic analysis, undertaken by the Information Technology Industry Council that considered the impact on European trade, explains the impact on EU GDP would be *negative 0.8-1.3%* if international data flow were seriously disrupted or stopped.[65] In Indonesia it has been shown that the impact on overall domestic investments would be *negative 2.3%* while exports would *decrease by 1.7%* as a direct loss of competitiveness.[66]

Many services popular with Indonesia's consumers and industries rely on the free flow of data across borders. Data residency requirements are harmful in that they inhibit market opportunities in Indonesia and constrain Indonesian users seeking access to markets and to useful services. Localization requirements limit the deployment of cloud services in Indonesia and constrain Indonesian enterprises seeking the benefits of cloud computing, as cross-border data flows enable market access through greater trade and can provide enhanced data security.

Restrictions on cross-border data flow create trade barriers and impact business models. These burdensome regulations can slow or prevent business transactions and international trade, which increases costs and obstructs the delivery of products to the market.[67] Countries that enact barriers to data flows make it harder and more expensive for their businesses to gain exposure and to benefit from the ideas, research, technologies, and best practices that accompany data flows and the innovative new goods and services that rely on data. Barriers to data flows also mean delays and higher costs in the development of new and innovative goods and services.[68]

7.4 Good International Practices

Data residency requirements do not adequately address the objectives of greater privacy protection and regulatory oversight. Privacy protection is best addressed by requiring a data

[63] The study uses a computable general equilibrium model (CGE) called GTAP8. The effect on productivity is created using a so-called augmented product market-regulatory index for all regulatory barriers on data, including data localization, to calculate domestic price increases or total factor productivity losses. Matthias Bauer, Hosuk Lee-Makiyama, Erik can der Marel, Bert Verschelde, "The Costs of Data Localization: Friendly Fire on Economic Recovery" (European Centre for International Political Economy, March 2014), http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.
[64] European Centre for International Political Economy, The Costs of Data Localization: Friendly Fire on Economic Recovery (March 2014), http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf
[65] http://www.itic.org/dotAsset/9/b/9b4cb3ad-6d8b-469d-bd03-b2e52d7a0ecd.pdf
[66] European Centre for International Political Economy, The Costs of Data Localization: Friendly Fire on Economic Recovery (March 2014), http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf
[67] Cisco Systems, By 2025, Internet of things applications could have $11 trillion impact (2016), http://www3.weforum.org/docs/GITR2016/WEF_GITR_Chapter1.2_2016.pdf
[68] Information Technology & Innovation Foundation, Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? (May 2017), http://www2.itif.org/2017-cross-border-data-flows.pdf

controller to locate data only in jurisdictions with similar legal protections. Regulatory oversight and law enforcement access should focus on jurisdiction over the data controller (through which access is provided) and the location of access and control, rather than the location of the data (where a regulator's access is often not possible either because of technical measures taken by the data controller or lack of legal authority).

Governments should encourage both private and public sector data classification as a means to align risk with the appropriate level of protection. Classifying data into discrete categories enables better-informed decisions to be made with regard to controls on access, storage and transmission of the data. Data classification aligns the safeguards required for different types of data, thereby reducing cost while ensuring the appropriate level of security.

Governments that have employed data classification have managed security risks, while providing flexibility to government departments and agencies to choose the most appropriate entity to manage their data.

- In the UK, the government uses a three-tier approach to data classification. Data is classified as official, secret and top secret, with 90% of government information being classified as official – the lowest security classification for their data. Commercially available products can be used to safeguard this level of data, at the same time bearing in mind robust and effective protections are put in place.
- A similar tier approach is applied in Singapore, with level 1, level 2 and level 3 data classification.

8. Opportunities for Reform

From a policy maker and regulator's point of view, the emergence of the digital economy changes the landscape. As business models and markets are transformed, the traditional industry-specific approach to policy setting will no longer enable expected economic growth and provide social development outcomes.

For regulators, the shift from being "risk managers" to becoming growth enablers is necessary as existing policy tools and regulatory regimes, developed for traditional business models, are found to be increasingly unsuitable for the new interconnected landscape of the digital economy.

With both regulators and policy makers in Indonesia facing multiple challenges in the face of the growing digital economy, the following areas are recommended for that prioritization:

1. Cross-sectoral collaboration;
2. Consumer protection; and
3. Data classification (to replace data localisation).

These issues also represent some of the biggest gaps in current policy approach between Indonesia and international best practices.

8.1 Cross-sectoral Collaboration

Traditional public administration functions are based on vertical silos – wherein public servants' expertise is focused upon specific policy domains (such as transportation, education or health) – and the legislative and regulatory frameworks in which they operate define and reinforce such focus. The digital economy requires the breaking down of such boundaries so that opportunities can be jointly targeted and managed and skillsets can be jointly applied.

Developing a whole-of-government framework enables and encourages agencies to move towards a more collaborative agenda. Such an approach needs to be both top-down and bottom-up. From the top, developing such a framework means that planning and resource allocation is done taking different constituencies into account. The Internet and related communications channels may be the enabling platform for growth, but that doesn't mean that the communications (or digital) agency knows how best to enable education sector growth. Similarly, education officials can be expected to understand what is required in their sector, but should not be expected to understand (a) the rollout of networks and accessibility, (b) the transformational potential of such network access, or (c) the skillsets required for a next generation of citizens growing up digital native. This last aspect is fundamentally important to preparing an economy for 21st century development and opportunity: if the next generation is not growing up learning, playing, transacting and bettering their health on digital networks, they will enter the workforce constrained, and the digital divide will have grown potentially insurmountable.

This top-down approach will also force a rethink in the role of regulators, increase the agility of government policy, and create ongoing opportunities for cross-agency learning and exchange of knowledge.

There is currently a lack of meaningful inter-agency collaboration in Indonesia, and a cross-sectoral approach to most economic issues is not employed – as has been illustrated with multiple contradicting regulations. In this context, a more bottom-up "piecemeal" approach to enablement should be adopted even as a more holistic framework is being developed. The lack of an existing framework for cross-sectoral planning should not be an excuse for targeting specific issues and specific developments now.

Other governments in the region have already chosen to create distinct entities to foster and coordinate the development of the digital economy, including the Ministry of Digital Economy and Societies (MDES) in Thailand, and the Malaysian Digital Economy Corporation (MDEC) in Malaysia, or specialized units within the Prime Minister's Office, to ensure sufficient political will.

- Singapore's GovTech, "the CIO of the Singapore government" in charge of the digital transformation of the public sector, established a cluster group that collaborates closely with sectoral agencies (in finance, health, education etc.) to ensure that newly developed digital services answer the needs of their users.[69]

It should be noted that specialized agencies alone won't create a cross-sectoral communication process without establishing formalized communication channels and collaboration methods.

8.2 Consumer Protection

There is significant overlap in consumer protection responsibilities across agencies in Indonesia and, as a result, much confusion for the consumer. There is a pressing need for regulators to work collaboratively on such issues, and to become clear on roles and responsibilities. There is also a lack of clarity on the various responsibilities and a lack of

[69] GovTech Singapore, Clusters Group, https://www.tech.gov.sg/About-Us/GovTech-Teams/Clusters-Group/Clusters-Group

leadership on where consumer protection issues should be brought. Each of these pressures are only going to increase as the digital economy grows.

It is recommended that agencies (such as the KPPU) establish working relationships with, for example, the Directorate of Consumer Empowerment (within the Directorate General Consumer Protection and Trade Order, Ministry of Trade).[70] Other agencies to be prioritized include the financial sector regulators, BI and OJK, Kominfo from the IT sector, and, as has been seen above, the Ministry of Transportation.

The general principle for decision-making should be based upon adopting a "functional approach" – wherein regulators are encouraged to treat comparable business models with equal risks the same way, and treat technology as a neutral factor when formulating regulations.

For example, in the digital economy, instead of regulating a digital service provider so that it becomes a traditional business model (i.e. regulating Go-Jek so that it becomes more like Blue Bird), minimum consumer protections should be implemented. This approach does not restrict innovation and growth in the digital economy.

- Singapore's Land Transport Authority (LTA) regulates private-hire car drivers from ride-hailing services (such as Uber and Grab) to protect commuter interests and safety. All drivers are required to hold a Private Hire Car Driver's Vocational License; undergo relevant training and pass requisite tests on road and passenger safety. Background screening is also conducted on all drivers.[71]

8.3 Data Localization

By developing and implementing a data classification scheme, the Government of Indonesia can ensure that appropriate controls are put in place for protecting sensitive data and for ensuring access to data with particular national sovereignty considerations. These requirements:

- ensure appropriate levels of security for government information;
- discourage inefficient allocation of resources and expensive security controls for less sensitive information;
- enable adoption of cloud computing; and
- improve data security.

They further provide a far more productive and nuanced approach to "localising" data that may be deemed essential to sovereignty than a blanket requirement for *all* data to be localised, and the attendant damage that this will bring to economic growth from the constraints placed on cross-border data flows.

Under such an approach data can be broadly divided into three tiers:

[70] Direktorat Pemberdayaan Konsumen, Direktorat Jenderal Perlindungan Konsumen dan Tertib Niaga Kementerian Perdagangan

[71] Land Transport Authority, New Regulations for Private Hire Car Drivers and Vehicles to Better Protect Commuter Interests https://www.lta.gov.sg/apps/news/page.aspx?c=2&id=59c466e2-8eff-46bc-8d60-f13bb00de4b2

- **Public Data,** which can be stored on accredited public cloud;
- **Tier 1 – Protected Data,** which can be stored on accredited public cloud;
- **Tier 2 – (Strategic) Restricted semi-sensitive data,** which can be stored on accredited public cloud or community cloud, with encryption requirements; and
- **Tier 3 – (Highly Strategic) Government confidential and above-sensitive data** which may require cloud deployment or accredited cloud infrastructure with a higher standard for specific encryption and data security requirements.

The Government of Indonesia should task an information security lead organization to develop guidelines and ensure proper security measures are implemented in a consistent manner across all agencies.

Australia Indonesia Partnership for Economic Governance

The Digital Economy in Indonesia

27 December 2017