9. ASEAN 2040: Data Flows and Electronic Payments

Mari Pangestu and Hosuk Lee-Makiyama

May 2019

This chapter should be cited as
Pangestu, M. and H. Lee-Makiyama (2019), 'ASEAN 2040: Data Flows and Electronic Payments', in Intal, P. and M. Pangestu, *Integrated and Connected Seamless ASEAN Economic Community*, Jakarta, ERIA, pp. 203–217.

ASEAN 2040: Data Flows and Electronic Payments

Mari Pangestu,
Universitas Indonesia

Hosuk Lee-Makiyama,
European Centre for International Political Economy (ECIPE)

Context of the Digital Economy until 2040

As e-commerce and the digital economy are increasingly subsuming every aspect of commercial and societal transactions, the Association of Southeast Asian Nations (ASEAN) integration process now includes the challenge to create its digital market. In that regard, data flows and online payments are the 'glue' that integrates all the other freedoms.

E-commerce already accounts for a market turnover that is equivalent to the gross domestic product of a G7 country, and more than half of today's trade in services is dependent on information and communication technology (ICT) infrastructure and data flows (United Nations Conference on Trade and Development (UNCTAD), 2011). Consumer banking, cross-border remittances, and payments are moving onto an entirely online environment. In addition, new concepts like digital manufacturing, 5G telecom networks, and artificial intelligence (AI) will make economies even more data-dependent.

Admittedly, 2040 is far off in the context of digital technology. Billions of goods, industrial and household equipment, devices, vehicles, and containers will be connected and go online in the coming decade alone. By 2040, all the ASEAN countries should have fully realised and implemented concepts like digital manufacturing, 5G, AI, or internet of things (IoT) – and will be on the path to the next step in societal and economic transformation. As technological cycles spin faster than political cycles, ASEAN cooperation must address, solve, and move past the issues that define the incumbent decade. By 2040, ASEAN countries will probably be in the midst of tackling the next-next generation of challenges.

Inevitably, this paper looks first and foremost to the policy concepts that are known today. The mobile internet technology took less than 10 years to complete. Cross-border data flows and online payments are likely to be forgone policy challenges by 2040, but policy analysts could not possibly be expected to answer the policy implications of the 6G technology that does not yet exist on engineers' drawing boards.

However, a prerequisite for digitisation is the free flow of data which allows for seamless communications, without regulatory frictions, and permits new and innovative services to enter into the uncharted and unregulated territory – occasionally making the existing regulatory systems obsolete.

Rather than resisting such changes, the path forward also includes managing the tensions within numerous policy disciplines, e.g. security, privacy, disruptions, competition, taxation, and regulatory agencies' capacities. Within regional cooperation forums like ASEAN, interoperability and standards of technologies and regulations within a country and between countries are essential. For example, as national privacy laws have not yet been implemented in all national legislative systems, interoperability and free data flows on the level of ASEAN are not yet developed.

However, unless ASEAN countries take the step towards national and regional frameworks, ASEAN cannot build its 2040 vision – not just in the digital economy. As trade in traditional goods and services moves online, the existing intra-ASEAN commitments (as well as ASEAN free trade agreements with third countries) will be rolled back unless they are supported by commitments to keep the digital economy open.

Point of Departure: Technology and Policy

Market assessments estimate the value of all commercial transactions conducted with consumers (B2C), business (B2B), and peer to peer (C2C) to have totalled $2.3 trillion in 2017, growing at 25% per year (eMarketer, 2018). In other words, if e-commerce were a sovereign economy, it would be equivalent to the size of India or the Russian Federation – and still grow four times faster than the Chinese economy (World Bank, 2016). While much of the turnover and growth takes place in Asia and the Pacific, the e-commerce market in ASEAN is still just a fraction of these volumes. However, Southeast Asia is the fastest growing region, with a growth rate that is seven percentage points above the rest of the world and six times faster than its offline equivalents – projected to reach $90 billion by 2025 (Google and Temasek, 2017; 2018).

Data traffic is also growing in the region, both in amounts and speeds (Table 1). Asia and the Pacific will overtake North America in terms of total data traffic by 2021 (Cisco, 2017). However, the regional growth is projected at a marginally higher compound annual growth rate than the global average, while the speeds (especially the critical mobile connection speeds) will neither outpace the rest of the world nor the increase in traffic.

The critical rollout of the mobile networks is central in this regard, especially as the ongoing upgrade of the mobile networks will make the difference between broadband and mobile indistinguishable. The 5G network services are assumed to start in 2018, and full national coverage will be completed in the Organisation for Economic Co-operation and Development (OECD) countries and China within less than 4 years (Weissberger, 2018; Bushnell-Embling, 2017).

Table 1: Projected Growth in IP Traffic and Connection Speeds by Region (CAGR, 2016–2021) (%)

Region	IP traffic increase	Fixed broadband speeds	Mobile connection speeds
Global	**24**	**14**	**24**
Asia Pacific	26	13	16
Latin America	20	17	27
North America	22	18	13
Western Europe	22	12	20
Central and Eastern Europe	21	9	24
Middle East and Africa	42	18	23

CAGR = compound annual growth rate, IP = internet protocol.

Source: Cisco (2017).

By industry projections, 28 billion IoT devices – mostly non-personal devices such as household goods, industrial equipment, and transport equipment – will go online in the early stages of 5G deployment, i.e. within a couple of years (Gartner, 2017).

In other words, 5G will be built and operational in much of ASEAN by 2022 or soon thereafter. If the telecom industry follows the same investment cycles of the past 3 decades, the technology that comes after 5G – the sixth generation (6G) networks, which have not yet been invented – should also be fully implemented by 2040. By then, 6G should have at least the reach of today's 4G in each of the ASEAN countries, while 5G should be as common as 2G/3G coverage. Therefore, even the most remote regions of today's developing countries will have access to speeds equivalent to 200 times those of 4G, 1,000 times better energy consumption, and 20 times better latency (IHS Economics and IHS Technology, 2017).

Such speeds and capacities enable a fully mobile consumer-centric digital economy across the region. However, 5G is also the first network that is primarily designed for commercial business and industrial application. The 5G networks will in turn enable the so-called fourth industrial revolution (aka Industry 4.0) – including digital supply networks, smart

factories, and digital manufacturing – which will fundamentally change traditional manufacturing, especially in light manufacturing like consumer goods, textiles and clothing, and motor vehicles (and their supporting services) which are essential for the ASEAN economies.

While we can be sure that the technical infrastructure will be built, the legislative framework for supporting data flows on today's and future infrastructure is critical for the commercial applications to evolve and disseminate. The importance of cross-border data flows is increasingly recognised in global business and international trade, but many regulatory impediments have already been implemented.

Trade on the internet is increasingly fragmented by government measures designed to disrupt the open exchange of data. To date, at least 36 jurisdictions have banned moving bits and bytes across borders, imposing partial or full data localisation requirements where the authorities require all information to be stored on servers within a jurisdiction (Lee-Makiyama, 2017). Such measures are typically imposed for privacy reasons, and the vast majority of all transfers (about 75% of all transmitted data) was already user-generated by 2012 (Tucker, 2013). All data transfers, without exception, contain some form of metadata (such as email addresses, phone numbers, or internet protocol (IP) addresses), and even non-personal information in the form of enterprise and operational data (e.g. technical readings of machinery, or stock inventory) stored within a corporate network contains information on personnel who are logged in while collecting, analysing, or transmitting data.

This means that any foreign business can be restricted from conducting business in another territory using privacy rules as a justification. Amongst the ASEAN countries, forced data localisation is already enforced in Brunei Darussalam, Indonesia, Myanmar, the Philippines, and Viet Nam through privacy rules or by other means. Malaysia and Singapore allow the transfer of personal information if certain conditions are fulfilled regarding the data processing or collecting entity, or the destination of the data. Brunei Darussalam, Cambodia, the Lao People's Democratic Republic and Malaysia lack privacy rules, while Thailand is currently drafting its laws (Table 2).

The use of online payments depends on a number of enabling policies in several challenging policy areas – not just cross-border data flows. Firstly, traditional consumer payment services required the liberalisation of banking, credit, and payment intermediation services. However, the distinction between these products is blurred because of the evolution of electronic payments – and today it is difficult to distinguish from telecommunications, or over-the-top or online processing services, as mobile payments are becoming stand-alone e-money or e-payment services (e.g. AliPay, M-pesa) without being linked to a bank account or credit card.

Table 2: Data Flow Restrictions in ASEAN

Country	Regulation
Indonesia	Economy-wide data localisation (Government Regulation No. 82 regarding the Provision of Electronic System and Transaction, 2012, with implementing acts, 2016); for online services (Electronic Information and Transactions Law, 2008)
Viet Nam	Full data localisation based on both privacy and national security laws (Decree No. 72/2013/ND-CP, Law 24 on Cybersecurity, 2018)
Malaysia	Data flows allowed under certain conditions (Personal Data Protection Act of 2010)
Philippines	Offshoring of financial data forbidden (under Resolution No. 2115 of 2015 - Amendments in the Manual of Regulations for Banks and Manual of Regulations for Non-Bank Financial Institutions on the guidelines on outsourcing)
Singapore	Data flows allowed under certain conditions (Public Data Protection Act, 2012)
Thailand	Draft legislation on privacy which would require specific consent by the data subject before an overseas transfer is executed.
Myanmar	No privacy legislation in place, but there are reports of how the government prefers data to be stored locally in some circumstances, and regulators may require on-site inspections.*
Brunei Darussalam	Brunei is alleged to have practices that require data generated within the country to be stored only in servers within the country.**
Lao PDR	The Lao PDR does not have privacy laws or any data flow restrictions.
Cambodia	Cambodia does not have comprehensive privacy laws. Although the right to privacy is a constitutional right, the regulations enforcing this right are in practice very narrow, e.g. the publication of the identity of minors by the press.

ASEAN = Association of Southeast Asian Nations, Lao PDR = Lao People's Democratic Republic.

Source: * Daniels (2017); ** Ezell et al. (2013).

To make online payment services available, technical infrastructure is required that consists of networks tying up point-of-sale locations (which may be using encrypted communication over the open internet), physical payment terminals, clearing facilities, etc. Such technical infrastructure may be controlled by a monopolist or a state-owned enterprise, which may be acting in a non-competitive manner. The complexity of this was illustrated by the 2012 World Trade Organization (WTO) dispute on electronic payment services (WTO, 2013).

Against this background, markets for carding, banking, and m-commerce are converging – a process which will surely be completed by 2040 – posing a challenge to the architecture of domestic regulation as well as regional cooperation.

Benchmarks in Regional Cooperation

As data protection is not yet implemented in all national legislative systems, common privacy standards, interoperability, and free data flows are understandably yet to be developed within ASEAN. There are, however, a few parallel developments that include some ASEAN members which could set the benchmark for future ASEAN rules.

In the area of privacy, a guideline is in place for privacy legislation and international transfers under Asia-Pacific Economic Cooperation (APEC) and its Cross-Border Privacy Rules (CBPR) on how member governments could implement their laws on a strictly opt-in basis (APEC, 2015). The countries opting into the system de facto recognise each other as essentially equivalent, while private entities from other areas can obtain a certification of compliance under which they may transfer data. By July 2018, only the United States, Japan, the Republic of Korea, and Singapore had opted in to recognise CBPR certification.

It is possible to envisage a similar normative guideline and model law system, supplemented by a certification system, within the ASEAN framework, or for the ASEAN members to incorporate the CBPR outright. For instance, the United States–Mexico–Canada Agreement (USMCA)

clarifies the level of protection that the parties must achieve on the protection of personal information by referencing the CBPR as well as OECD (Article 19.8, item 2), with legislative concepts that should be considered in domestic privacy legislation (Article 19.8, item 3).[1]

On cross-border data flows, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) binds a subset of ASEAN members (e.g. Malaysia, Singapore, and Viet Nam). It updates the existing WTO rules by protecting data flows, and data localisation measures, as barriers. The parties shall allow for 'cross-border transfer of information by electronic means' (Article 14.11). In addition, the CPTPP bans its parties from imposing data localisation requirements that 'require a covered person to use or locate computing facilities in that Party's territory' (Article 14.13).

This pair of provisions exempts domestic regulations that serve a *legitimate public policy objective*, given that the restrictions pass a two-tier test through *legitimacy* (no 'arbitrary or unjustifiable discrimination' or 'disguised restriction')[2] and *proportionality* (not 'greater than are required to achieve the objective').[3] Such exceptions correspond to the catalogue of cases for exceptions (albeit with slightly different wordings) under WTO rules granted for a limited set of objectives compared with the CPTPP's unspecific exemption for any legitimate objective,[4] while the CPTPP also exempts the entire financial industry from these provisions,[5] and is therefore inapplicable to online payments.

Such carveouts in the CPTPP are as extensive as the WTO rules, e.g. Viet Nam amended its data localisation requirements in June 2018 by invoking national security objectives in its Law No. 24 on Cybersecurity, 2018,[6]

---

1 Article 19.8.3 mentions the limitation on data collection, choice, data quality, purpose specification, use, security safeguards, transparency, individual participation, and accountability.

2 CPTPP Article 14.11 3(a) paraphrases the WTO two-tier test under the General Agreement on Trade in Services (GATS) Article 14 and the General Agreement on Tariffs and Trade (GATT) Article 21.

3 ibid.

4 GATS, Article 14. For a legal discussion on WTO exceptions and the digital economy, see Erixon, Hindley, and Lee-Makiyama (2009).

5 Definitions under the CPTPP Article 14.1.

6 See also Nikkei Asia Review (2018).

despite its intention to ratify the CPTPP. Minor semantic changes in the USMCA also improved its commitments: Where the CPTPP merely states that parties 'shall allow' data flows, the USMCA states 'no Party shall prohibit or restrict' data flows. Thus, mere *restrictions* (e.g. governments slowing down or complicating access to data) are now also within the scope of the cross-border data discipline – not just outright *prohibitions*. The USMCA removes the exceptions for legitimate policy objections for data localisation – in other words, there may be legitimate reasons to limit data flowing in and out of a country (including privacy protection), but no justifications to force businesses to use local ICT infrastructure to conduct business in a country.

Other impediments to data flows also exist, e.g. upstream and downstream anti-competitive behaviour against innovations. Without net neutrality provisions, telecom providers may selectively block or restrict data used by any service transmitted or online payments conducted on its network. Singapore is one of the few jurisdictions in the world that since 2011 bans operators from blocking legitimate online content and forces them to comply with antitrust and interconnection rules.[7]

Aside from the potential anti-competitive behaviour of telecom operators, other types of dominant market players (such as banks, retailers, and technology vendors) may abuse their dominance through their ability to set and enforce industrial standards while excluding smaller competitors. There are also filtering and blocking practices by governments which may be imposed for commercial reasons (e.g. to protect state-owned enterprises or national champions) as well as to ensure the full political authority of the internet (Erixon, Hindley, and Lee-Makiyama 2009). In sum, an ASEAN single market for the digital economy will depend on freeing data and payments through antitrust disciplines against private actors as well as all the layers of services liberalisation, including banking, cloud and data flows, and access to intermediaries or public telecommunication networks.

[7] Implemented by the Infocomm Media Development Authority in 2011.

New Challenges from Digitalisation

As new technology affects productivity – and different economies have a different rate of technological adoption – new disruptive technology must theoretically lead to a change in nations' comparative advantages. Such an impact of internet technologies has been established on both firm- and economy-wide levels (van Ark, 2016; OECD, 2015). However, new market entrants that do not carry over old legacy costs of old technologies or have exploited the economies of scale in global demand have threatened local monopolies, state-owned enterprises, and other sensitive stakeholders, especially in sectors like banking, retail, and media. The internet has changed the political economy in the industrial sectors it has disrupted. The impact of digitalisation will become more pronounced in other sectors (including manufacturing) until 2040, and industrial policy responses or protectionist responses cannot be precluded.

The internet and the digital economy are also challenging the regulator outright. A widely spread misconception is that internet commerce takes place in no man's land. In reality, the digital economy is actually subject to overlapping (and often contradictory) rules as governments compete to exercise their jurisdiction extraterritorially, contravening the territoriality principle of international law (Lee-Makiyama, 2013). Restrictions by the regulator must be overcome by 'passporting' and adequacy solutions (similar to how the European Union privacy rules or financial services operate), which allow foreign businesses from essentially equivalent legal systems to operate in the economy.[8]

Meanwhile, the openness of the digital economy makes the authority of the national regulator against certain opinions, activities, or services more difficult to uphold. Such policy challenges require either normative legal prescription and harmonising of penal codes within ASEAN, or law enforcement cooperation under mutual legal assistance treaties between countries when an entity provides a service that is illegal in another country (Lee-Makiyama, 2013). While harmonisation of penal codes may

[8] Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

be impractical, ASEAN has signed the Treaty on Mutual Legal Assistance in Criminal Matters, which has been in force since 2004.[9]

Fiscal policy is another area where e-commerce and online payments are already presenting a challenge. There is no evidence of tax bases in the ASEAN countries eroding (Ferracane and Lee-Makiyama, 2017). Instead, the dissemination of online payments leads to an increasing share of the informal ('grey') economy becoming formalised and properly taxed. Numerous unilateral and international initiatives address the problem, including the OECD base erosion and profit shifting,[10] the European Union digital service tax,[11] and United States taxes on profit shifting (global intangible low-taxed income).[12] In addition, by 2040, fiscal revenues may be forgone from 3D printing and other new emerging technologies not yet on the horizon.

Finally, increased digitalisation and cross-border transactions raise the issue of national and cyber security. National security concerns have already affected the open trading system where certain suppliers of network equipment, cloud services, control systems, and data processing (including payment and purchase history) are routinely excluded. Government regulations restricting digital trade and the use of data in these sectors are increasing – and ASEAN must decide whether to explore new areas of cooperation in the form of common cybersecurity standards, or even invest in joint cyber defence capabilities. Further, cyber espionage is increasingly lucrative as the value of intangibles and trade secrets on corporate clouds is increasing exponentially (Lee-Makiyama, 2018). Without proper cybersecurity measures, the number of ways to exploit the vulnerability of critical infrastructure is increasing. Simultaneously, what is deemed 'critical infrastructure' includes an ever-increasing number of sectors, e.g. telecom, transport and energy infrastructure, financial institutions, marketplaces, government, and public services.

---

9 ASEAN Treaty on Mutual Legal Assistance in Criminal Matters, 2004.

10 OECD Multilateral Convention to Implement Tax Treaty Related Measures to Prevent Base Erosion and Profit Shifting, 2017.

11 European Commission Proposal for a Council Directive laying down rules relating to the corporate taxation of a significant digital presence, COM(2018) 147 final.

12 US Congress, Tax Cuts and Jobs Act, 2017 (115-97).

Conclusions

Data flows, innovative applications, and new high-speed networks are underpinning the new industrial revolution – industry 4.0 – or much broader societal concepts like Society 5.0.[13] These industrial and societal ideas should be fulfilled within ASEAN by 2040 through national policy initiatives, private investments, and open market demand. The upgrade of the digital economy nationally will enable regional cooperation within ASEAN in many areas. The ASEAN dimension will leverage and underwrite the digital dividend for its members.

Innovative use of data and payment systems will bring new products and services to more people in ASEAN and allow them to trade more efficiently within the region as well as globally. Moreover, freer flow of data and payments can harness the social benefits for small and medium-sized enterprises, expand the fiscal base, and help the region's migrants through low-cost processing of payments for remittances. Such benefits are hinged on justice and home affairs cooperation (especially in the area of privacy), service liberalisation, cybersecurity standards, reviewing fiscal policy, and a multitude of other policy areas.

The region is also supplemented by competing frameworks, e.g. the APEC CBPR and trade disciplines under the CPTPP. In the absence of its own certification framework for privacy and data flows within ASEAN (e.g. in the 2018 E-Commerce Agreement or the 2025 Work Programme), ASEAN members may instead adopt unilateral policies (similar to those of the European Union or China on data privacy; or the European Union on international taxation), forfeiting a digital ASEAN Single Market – or regional cooperation altogether.

[13] Government of Japan, Cabinet Office, Society 5.0. http://www8.cao.go.jp/cstp/english/society5_0/index.html (accessed 7 October 2018).

References

APEC (2015), *APEC Privacy Framework*. Singapore: APEC Secretariat.

Bushell-Embling, D. (2017), 'Japan's cellcos to invest over $45.5b in 5G', Telecom Asia, 8 June.

Cisco (2017), The Zettabyte Era: Trends and Analysis. Available at: https://www.cisco.com/c/en/us/solutions/collateral/service (accessed 7 October 2018).

Daniels, J. (2017), 'IT Laws and Regulations in Myanmar: 5 Key Points to Consider', Blog, Baker McKenzie, 29 November.

eMarketer (2018), *Worldwide Retail and Ecommerce Sales: eMarketer's Updated Forecast and New Mcommerce Estimates for 2016–2021*. New York, NY: eMarketer.

Erixon, F., B. Hindley, and H. Lee-Makiyama (2009), 'Protectionism Online: Internet Censorship and International Trade Law', *ECIPE Working Paper*, No. 12. Brussels: European Centre for International Political Economy (ECIPE).

Ferracane, M.F. and H. Lee-Makiyama (2017), 'The Geopolitics of Online Taxation in Asia-Pacific: Digitalisation, Corporate Tax Base and the Role of Governments', *ECIPE Policy Briefs*, No. 2. Brussels: ECIPE.

Gartner (2017), *Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 2016*. Stamford: Gartner.

Google and Temasek (2017), *e-Conomy SEA Spotlight 2017: Unprecedented growth for Southeast Asia's $50B internet economy*. Singapore: Google, Temasek.

Google and Temasek (2018), *e-Conomy SEA 2018: Southeast Asia's internet economy hits an inflection point*. Singapore: Google, Temasek.

IHS Economics and IHS Technology (2017), *The 5G economy: How 5G technology will contribute to the global economy*. London: IHS.

Lee-Makiyama, H. (2013), 'A Multilateral Legal Assistance Protocol: Preventing Fragmentation and Re-territorialisation of the Internet', *ECIPE Policy Briefs*, No. 9. Brussels: ECIPE.

Lee-Makiyama, H. (2017), 'The digital trade oversight: How ignoring the internet opened a backdoor to de-globalization', *International Trade Forum*, Geneva: International Trade Centre, 10 July.

Lee-Makiyama, H. (2018), 'Stealing Thunder: Cloud, IoT and 5G will Change the Strategic Paradigm for Protecting European Commercial Interests. Will Cyber Espionage be Allowed to Hold Europe Back in the Global Race for Industrial Competitiveness?', *ECIPE Occasional Papers*. Brussels: ECIPE.

Nikkei Asia Review (2018), 'Vietnam's cybersecurity law sparks concerns from businesses', Available at: 12 June. https://asia.nikkei.com/Politics/Vietnam-s-cybersecurity-law-sparks-concerns-from-businesses (accessed 7 October 2018).

OECD (2015), *The Future of Productivity*. Paris: OECD.

Tucker, P. (2013), *'Has Big Data Made Anonymity Impossible?', MIT Technology Review*, 7 May. Boston, MA: Massachusetts Institute of Technology.

UNCTAD (2011), *Information Economy Report 2011: ICTs as an Enabler for Private Sector Development*. Geneva: UNCTAD.

van Ark, B. (2016), 'The Productivity Paradox of the New Digital Economy', *International Productivity Monitor*, 31, pp.3–18.

Weissberger, A. (2018), 'CCS Insight: China to lead global 5G adoption which will take longer than 4G, IEEE Communications Society', 24 January. http://techblog.comsoc.org/2018/01/24/ccs-insight-china-to-lead-global-5g-adoption-which-will-take-longer-than-4g/ (accessed 7 October 2018).

World Bank (2016), *World Development Indicators 2016*. Washington, DC: World Bank. http://wdi.worldbank.org (accessed 7 October 2018).

WTO (2013), *China – Certain Measures Affecting Electronic Payment Services*, DS413. Geneva: WTO.