Technology, Media, And Telecommunications

Technology, Media and Telecommunications Regional Update: A Recap from May 2017 to December 2017

Contents

Introduction

Looking back on the year 2017, we are very excited to share with you the significant legal developments in the technology, media and telecommunications ("**TMT**") sector during the third and fourth quarters of 2017. This update aims to highlight the significant TMT-related legal developments in the ASEAN region, as well as in the key economies across the world.

As always, we are excited to provide you with this helpful recap of key developments, and more, in ASEAN and further afield. As with our previous regional updates, these quick summaries have been prepared by our TMT practitioners in the Rajah & Tann Asia Network, which spans nine countries in the ASEAN region. If you or your business partners wish to find out more about any of the updates here, please do not hesitate to reach out to any of our regional offices in Rajah & Tann Asia. Without further ado, here are your updates.

Technology, Media, And Telecommunications

RAJAH & TANN ASIA NETWORK

SINGAPORE

PDPC Launches Public Consultation Exercise on Proposed Revisions to the PDPA

The Personal Data Protection Commission ("**PDPC**"), on 27 July 2017, issued a public consultation paper regarding its proposed review of the Personal Data Protection Act 2012 ("**PDPA**"). The following amendments to the PDPA were proposed:

(a) Providing parallel bases for collecting, using, and disclosing personal data. This alternative to the consent regime takes into account circumstances where it may be impractical, or where it may not be desirable or appropriate, to obtain consent. Organisations will be required to undertake a risk and impact assessment if seeking to rely on this alternative regime; and
(b) Imposing a mandatory data breach notification obligation. The PDPC proposed to require organisations to notify the PDPC and/or affected individuals if the organisation has experienced a data breach, depending on the nature of the breach.

Interested parties were invited to submit their views by 5 October 2017. A total of 62 responses were received by the PDPC as at 5 October 2017. At the time of writing, the PDPC has not released its responses to this consultation exercise.

PDPC Issues EU GDPR Factsheet for Organisations

The PDPC issued a factsheet on the European Union General Data Protection Regulation ("**EU GDPR**") on 4 October 2017, highlighting key aspects of the EU GDPR that may be applicable to organisations in Singapore.

The PDPC notes that the EU GDPR will apply to an organisation established outside of the EU, so long as the organisation offers goods or services to individuals in the EU, or monitors their behaviour within the EU.

Depending on the provisions that are infringed upon, organisations that do not comply with the EU GDPR may be subject to administrative fines of up to EUR 20 million or 4% of worldwide annual turnover of the preceding financial year, whichever is higher.

PDPC Launches Public Consultation Exercise on Proposed Advisory Guidelines for NRIC Numbers

On 7 November 2017, the PDPC invited the public to provide feedback on the proposed advisory guidelines on the PDPA for National Registration Identification Card ("**NRIC**") numbers. The public consultation exercise ran from 7 November to 18 December 2017.

The PDPC is of the view that special considerations should be given to the collection and use of NRIC numbers "*as the NRIC number is a permanent and irreplaceable identifier which can be used to unlock large amounts of information relating to an individual.*" Additionally, it was highlighted that the indiscriminate collection and use of NRIC numbers increases the risk that individuals' NRIC numbers may be used for illegal activities such as identity theft and fraud. Accordingly, the PDPC is proposing to revise the existing advisory guidelines regarding NRIC numbers, and to issue a technical guide that provides guidance on the alternatives that can be considered in place of the NRIC number.

Technology, Media, And Telecommunications

Planned Investment of up to S$150 million in AI capabilities

During the Innovfest Unbound conference held in May 2017, Dr Yaacob Ibrahim, the Minister for Communications and Information, unveiled AI.SG – a national programme to boost Singapore's artificial intelligence ("**AI**") capabilities. The National Research Foundation, a partner of the programme, will invest up to S$150 million over 5 years in AI.SG.

AI.SG will be applied to three focus areas, namely finance, city management solutions, and healthcare, seeking to achieve the following:

(a) Using AI to address major challenges that affect society and industry;
(b) Investing in deep capabilities to catch the next wave of scientific innovation; and,
(c) Broadening adoption and use of AI and machine learning within industries.

Marvelstone Group to launch AI Hub in Singapore

It was announced on October 2017 that Marvelstone Group, a private investment firm, plans to launch an artificial intelligence ("**AI**") hub in Singapore in 2018. The planned hub seeks to incubate 100 AI start-ups per year and to build intellectual property in the area of AI.

Aligning with the Singapore Government's Smart Nation vision, the AI hub seeks to serve the existing need in the market, and also to position Singapore as a global leader in AI technologies. In this regard, the AI hub aims to be an AI incubator to attract innovative AI start-ups, providing support as well as helping commercialise the start-ups' products.

MCI and CSA Launch Public Consultation Exercise on Cybersecurity Bill

On 10 July 2017, the Ministry of Communications and Information ("**MCI**") and the Cyber Security Agency of Singapore ("**CSA**") invited the public to provide feedback on the proposed Cybersecurity Bill (the "**Bill**"). The public consultation exercise ran from 10 July to 24 August 2017.

It is proposed for the Bill to establish a framework for the oversight and maintenance of national cybersecurity in Singapore, and to empower the CSA to carry out its functions. These will be achieved through the Bill's four objectives:

(a) Formalising the duties of critical information infrastructure ("**CII**") owners, which includes spelling out the CII owners' responsibilities in protecting their respective CII, and a cybersecurity incident notification obligation;
(b) Empowering CSA to manage and respond to cybersecurity threats and incidents expediently;
(c) Creating a framework of information sharing for purposes of preventing, detecting, countering, or investigating any cybersecurity threat or incident; and
(d) Introducing a licensing framework for regulating selected cybersecurity service providers.

The public consultation exercise garnered 92 submissions. On 13 November 2017, the CSA issued a statement, informing that the MCI and CSA intend to refine several aspects to the Bill, which may include:

(a) Clarifying on the proposed definition of CII;

(b) Taking into account of sectoral requirements when imposing duties on CII owners; and
(c) Simplifying the proposed licensing regime.

The Bill is slated to be tabled in Parliament in 2018, according to Dr Yaacob Ibrahim in his speech during the 2nd ASEAN Ministerial Conference on Cybersecurity held in Singapore on 18 September 2017.

SingCERT Issues Alert on Major Wi-Fi Flaws that May Expose Users to Cyber Attacks

Multiple security flaws of the Wi-Fi Protected Access 2 protocol ("**WPA 2**") were exposed by researchers on 16 October 2017. Upon such disclosure, the Singapore Computer Emergency Response Team ("**SingCERT**") issued an alert on 17 October 2017, detailing the potentially affected systems, impact of the security flaws, as well as recommendations to mitigate the risk.

The impact of these flaws is widespread; typically, devices connected using WPA or WPA 2 may be vulnerable, whether such is used in homes or in offices. In addition to suggesting that users patch their operating systems, SingCERT recommended users to secure their networks using secondary encryption solutions such as a Virtual Private Network, or through the using of wired LAN for internet connection.

Regional Centre Established in Singapore to Help Combat Cybercrime

The Monetary Authority of Singapore, together with the Financial Services Information Sharing and Analysis Center ("**FS-ISAC**") launched the FS-ISAC Asia Pacific Regional Analysis Centre's (the "**Centre**") office and operations in Singapore on 14 November 2017. Supporting 49 financial institutions across nine Asia Pacific countries, this collaboration will aid the Asia Pacific countries in dealing with cross-border cybercrime more effectively. The nine Asia Pacific countries are Australia, India, Japan, Malaysia, New Zealand, Singapore, South Korea, Taiwan and Thailand.

The Centre provides 24/7 local and global coverage with threat information sharing, actionable intelligence, as well as tools and resources to respond to incidents. Additionally, members of the Centre may also benefit from webinars, cybersecurity trainings, and summits, which may be held from time to time. The next FS-ISAC Asia Pacific Summit will take place in Singapore on 17-18 July 2018.

MAS Clarifies Regulatory Position on the Offer of Digital Tokens in Singapore

Amid the rise of initial coin offerings ("**ICOs**"), the Monetary Authority of Singapore ("**MAS**") has clarified on 1 August 2017 that the offer or issue of digital tokens in Singapore will be regulated by the MAS if the digital tokens constitute products regulated under the Securities and Futures Act (Cap. 289). Such clarification came after the US Securities and Exchange Commission issued an investigative report on 25 July 2017 on whether the DAO (a virtual, digital Decentralised Autonomous Organisation that is instantiated on the Ethereum blockchain) had violated federal US securities laws with unregistered offers and sales of DAO Tokens in exchange for "Ether," a virtual currency.

A key concern of the MAS regarding such digital token and virtual currency-related investment schemes is the lack of understanding of the risks involved in such schemes. As such, the MAS, collectively with the Commercial Affairs Department, issued an advisory note on 10 August 2017 informing the public about certain risks they should look out for when considering whether to invest in such schemes.

The topic of cryptocurrency use in Singapore, as well as whether the MAS intends to regulate ICOs, has since been raised in Parliament on 2 October 2017. On 14 November 2017, the MAS issued a Guide to Digital Token Offerings

to provide further guidance on the application of securities laws in relation to offers or issues of digital tokens in Singapore.

MAS Establishes Payment Council to Realise E-Payments Society

The Monetary Authority of Singapore announced on 2 August 2017 that it will establish a Payments Council as an initiative to realising the vision of an e-payments society in Singapore. A taskforce was set up by the Payments Council on 11 August 2017 to establish interoperable electronic payments. It was advocated by the Payments Council members that developing a common QR code for Singapore may be a practical and convenient way to introduce e-payments to cash-based merchants.

The taskforce aims to have in place the standardised specifications for the common QR code, to accept both domestic and international payment schemes, by the end of 2017.

National Day Rally 2017: Push for Smart Nation Initiatives

During the National Day Rally held on 20 August 2017, Prime Minister Lee Hsien Loong ("**PM Lee**") mentioned the initiatives and projects implemented towards building a Smart Nation. Specifically, PM Lee commented on the lack of unification of the current e-payment systems in Singapore, resulting in inconvenience to consumers and high costs for businesses. In this regard, it was mentioned that Singapore is working to implement a simple e-payments system usable throughout the nation.

PM Lee also unveiled plans and initiatives taken to work towards the Smart Nation vision, including the building of an integrated national sensor network, allowing security forces to analyse the combined data so that they can assess a situation quickly, respond promptly, or even pre-empt incidents and prevent them from occurring.

IMDA Requests for Public Consultation on 5G Mobile Services and Networks

On 23 May 2017, the Infocomm Media Development Authority ("**IMDA**") invited the public to provide feedback on developments relating to fifth generation mobile networks ("**5G**") and the spectrum required to run them. The public consultation exercise ran from 21 May to 21 July 2017, and received a significant number of submissions from industry experts.

The feedback received from the public consultation exercise would assist the IMDA in developing the necessary policies to facilitate the deployment of 5G technology. At the time of writing, the IMDA has yet to release their comments in relation to the public consultation. In order to facilitate industry players' understanding of how 5G will work in a real world environment, the IMDA has also waived frequency fees for testing of 5G technology. The 5G frequency fees have been waived up till 31 December 2019.

SingNet Fined for Fibre Broadband Service Disruption

Due to a fibre broadband service disruption which occurred on 3 December 2016, the IMDA found SingNet Pte Ltd ("**SingNet**") to be in contravention of the Code of Practice for Telecommunication Service Resiliency 2016. The IMDA, on 16 October 2017, imposed a financial penalty of S$500,000 on SingNet for this breach.

During the incident, which lasted nearly 24 hours and affected close to 90% of SingNet's subscribers, it was revealed that SingNet had failed to take prompt action to address the high utilisation loads before the incident, when

there were already warning signs in the lead-up to the incident. IMDA found that SingNet should have exercised greater due diligence and caution in preventing the overloading of its Dynamic Host Control Protocol servers.

The IMDA took into consideration mitigating factors when determining the quantum of the financial penalty. These factors included the offering of compensation to affected customers, the taking of preventive measures to avoid a recurrence of a similar incident, and the close co-operation with the IMDA during the investigation process.

MALAYSIA

Regulatory Authorities Probe Massive Data Breaches Involving Personal Data of Millions of Malaysians

On 19 October 2017, regulatory authorities in Malaysia, including the Malaysian Communications and Multimedia Commission ("**MCMC**") and the Personal Data Protection Commissioner's office ("**PDPC**"), were alerted to reports of a probable data breach through a popular online public forum, *lowyat.net*, in Malaysia. The illegally-obtained personal data of millions of Malaysians were listed for sale on the online public forum by an unknown source.

Reports stated that the data being sold was obtained from databases of several large operators in the telecommunications sector, job listings and recruitment websites, as well as several medical and dental associations in Malaysia. The data is said to consist of personal information such as individuals' names, mobile numbers, addresses and their national identification numbers, and the breach was believed to have occurred in 2014. The MCMC, PDPC and Malaysian police force are currently investigating the alleged data breach.

In a separate incident, on 13 November 2017, CIMB Group Holdings Bhd, a large and established banking institution in Malaysia, announced that it has recently heightened its information security measures amidst reports that several magnetic tapes containing back-up customer data were physically lost in transit during routine operations. In response to this incident, CIMB has temporarily suspended some services via its call centre, such as change of personal particulars for banking/credit cards and third party fund transfer or payment for customers. CIMB has reported the incident to Bank Negara Malaysia (the Malaysian Central Bank) and the police and investigations are underway.

Bank Negara Malaysia and Securities Commission Malaysia to Regulate Use of Cryptocurrencies in Malaysia

Bank Negara Malaysia ("**BNM**") (the Malaysian Central Bank) has announced that it will be issuing guidelines on cryptocurrencies by the end of the year. The BNM governor, Tan Sri Muhammad Ibrahim, said that the guidelines will also include anti-money laundering and terrorist financing practises for those who want to participate in the sector.

BNM previously released a statement in January 2014 that bitcoin (the current leading cryptocurrency) is not recognised as a legal tender in Malaysia. On 7 September 2017, the Securities Commission Malaysia ("**SC**") also issued a statement warning investors to be mindful of the potential risks involved in digital token based fundraising activities / investment schemes in Malaysia and elsewhere, which may be referred to as "initial coin offerings", "initial token offerings", "token pre-sale", or "token crowd-sale".

On a related note, the SC has also recently announced that it will likely unveil a framework on cryptocurrency in the coming months, alongside BNM. The SC is reviewing relevant regulations and guidelines to facilitate functional and

effective use of digital assets in the capital market, which include the secondary market trading of established cryptocurrency and digital assets.

Bank Negara Malaysia Issued Exposure Draft on Outsourcing Arrangements for Financial Institutions

On 28 September 2017, BNM issued an exposure draft of the proposed revised prudential framework on outsourcing arrangements for financial institutions (the "**Exposure Draft**"). The Exposure Draft, once it is finalised and comes into force, will be applicable to licensed banks, investment banks, Islamic banks, insurers / takaful operators, and prescribed development financial institutions.

The Exposure Draft aims to ensure that risk management practices for outsourcing arrangements by financial institutions remain effective moving forward amid intensification of technological advances in a more globalised and digitised environment. BNM invited written feedback from the public on the Exposure Draft, including suggestions on areas to be clarified and alternative proposals that BNM should consider. The period for submissions has since closed.

The material terms in the Exposure Draft are several, but some of the more material provisions require financial institutions to obtain BNM's written approval before entering into a new outsourcing arrangement or prior to renegotiating/renewing an existing outsourcing arrangement, as well as requiring that all outsourcing arrangements must be subject to a limited contractual period (presently suggested to be fixed at a maximum of 3 years).

Government of Malaysia Proposing to Amend the Goods and Services Tax Act 2014 to Tax Major Online Business Platforms

The Director General of Customs has announced that the Customs Department aims to amend the Goods and Services Tax Act 2014 to enable the Malaysian government to collect taxes from foreign companies operating in Malaysia within the digital economy.

The proposed amendments are intended to create a level playing field among companies operating in the country, and to "*reduce the imbalances between digital and non-digital transactions*". The Customs Department is studying ways to tax foreign online platforms, as at present the Malaysian government does not have the mechanisms required to impose such taxes.

Naming targeted companies such as Uber, Airbnb, Grab, Amazon and Google, the Finance Ministry clarified that the proposed amendments are intended to tax major foreign digital platform providers operating in Malaysia, and not small-time online businesses.

Government of Malaysia to Amend Gambling Laws to Address Online Gambling

The Deputy Prime Minister of Malaysia ("**DPM**") has announced that the Malaysian government is currently looking into proposed amendments to the Common Gaming Houses Act 1953 ("**CGHA**") to combat illegal gambling activities, including those carried out online.

The DPM, who is also the Home Minister, expressed that amendments to the CGHA are required as the CGHA was enacted during a time when online gambling and cyber gaming did not exist, and also considering that online gambling activities can now be carried out via smartphones. In a statement to the Dewan Rakyat (the Malaysian

House of Representatives) earlier in 2017, the DPM indicated that one of the amendments to online gambling laws would be to introduce heavier penalties on offenders.

Presently, the Home Ministry and Royal Malaysian Police are working closely with the Attorney-General's Chambers to determine whether it will be sufficient to amend the CGHA, or whether a new preventive law will have to be formulated specifically to address online gambling activities.

Malaysian Home Ministry to Formulate CCTV-related Laws

The Home Ministry has announced that they are in the midst of formulating CCTV-related laws to control and expand the use of the same in Malaysia.

According to the Deputy Home Minister, the new law will be aimed at increasing security as well as preventing and recording crimes occurring in public places, and further stated that the Home Ministry is considering making the installation of CCTV systems compulsory.

The new law will also address other specifications for the installation of CCTV systems, such as the requirement of having the system connected to the nearest police station, specifications on image quality, and the need for face detection software based on the police or the National Registration Department ("**NRD**") records.

In addition to the introduction of a new law, the Home Ministry is also set to introduce an auto tracking CCTV system, which will channel video feeds directly to the police and other enforcement agencies in order to aid them in tracking down suspects based on real-time visuals. The system will be installed in about 200 crime hotspots nationwide within the next two years, as part of the government's bid to digitalise assets and operations of the police in combating crime through modern policing.

INDONESIA

National Payment Gateway Finally Established

A few months before the 5-year anniversary of Government Regulation No. 82 of 2012 on Implementation of Electronic Transactions and Systems, including the obligation under its Article 43 (1) on the utilization of the national payment gateway for transactions involving more than one Electronic System Organizers, Bank Indonesia finally provides its guidance on national payment gateway by enacting Bank Indonesia Regulation No. 19/8/PBI/2017 on National Payment Gateway.

Prior to the national payment gateway regulation, electronic transactions in Indonesia were obliged to use a so-called national payment gateway if they involved more than 1 electronic system provider. However, this national payment gateway was not elaborated on then.

Now, under the national payment gateway regulation, it is clear that the national payment gateway is a system which consists of standard, switching, and services functions based on a set of rules and arrangement to nationally integrate payment instruments and channels. It has 2 main objectives: (i) interconnectivity of all existing payment channels, and (ii) interoperability of various payment instruments which are currently existing and used in Indonesia.

The national payment gateway will be organized by 3 main parties:

(a) The standard institution, which will prepare, develop, and manage standardized technical and operational specifications for the interconnectivity and interoperability of payment instruments, payment channels, switching, and the overall security of the payment system under the guidance and supervision of Bank Indonesia;
(b) Switching institutions, which will domestically process the payment transaction data for interconnectivity and interoperability of the payment system. For this purpose, all switching institutions are obliged to cooperate with at least two other switching institutions and their cooperation is subject to specific standards set by Bank Indonesia; and
(c) Services institutions, which are essentially tasked to manage the services provided to fulfil the needs of the retail payment system industry in the national payment gateway ecosystem.

The national payment gateway will connect Indonesian issuers, acquirers, payment gateway providers, as well as other parties which are deemed relevant by Bank Indonesia, with the ultimate objective of increasing non-cash transactions in Indonesia and actualizing the independency of Indonesia's national payment system, especially in respect of all financial transactions carried out in Indonesia.

Technical Provisions on Peer-to-Peer Lending to be Issued

In late 2016, the Financial Services Authority issued a regulation on peer-to-peer lending, effectively providing certainty and government support for the development of Indonesia's technology-based peer-to-peer lending industry.

The peer-to-peer lending regulation sets out comprehensive provisions on both peer-to-peer service providers as well as their users, including the provisions that must be present in the agreement between lenders and borrowers. More importantly, the peer-to-peer lending stipulates wide-ranging requirements with regard to the information technology system used by peer-to-peer service providers, including the requirement to place their data centre and disaster recovery centre in Indonesia (data localization requirement) as well as having sufficient security measures.

The Financial Services Authority has recently issued their draft on the implementing instrument to the peer-to-peer regulation, which sets out the technical provisions related to peer-to-peer lending, including:

(a) Registration process of users to a peer-to-peer lending service;
(b) Know-your-customer principle related provisions, requiring peer-to-peer lending service providers to carry out several obligations in order to ascertain the identity of their users;
(c) Loan request procedure, which consists a number of obligations that must be conducted by the peer-to-peer lending service provider including carrying out a credit worthiness check of the user in question;
(d) Contract standards for peer-to-peer lending, including the contract between borrowers and lenders, lenders and peer-to-peer lending service providers, as well as peer-to-peer lending service providers and banks (with respect to the use of escrow accounts and virtual accounts); and
(e) Risk mitigation that must be fulfilled by peer-to-peer lending service providers, including know-your-customer principle implementation, document checking, and user inquiry for any inaccurate information submitted.

The above draft of the peer-to-peer circular letter which will implement the peer-to-peer regulation was open to public inquiry from 30 October 2017 to 10 November 2017 and is now in the process of further harmonization and finalization.

Technology, Media, And Telecommunications

E-Commerce Building Blocks

In preparing to introduce its first e-commerce regulation, the Indonesian government enacted the e-commerce roadmap under Presidential Regulation No. 74 of 2017 on E-Commerce Roadmap, which aims to provide strategic guidance for and synchronize the efforts of the government to support and accelerate the development of e-commerce in Indonesia.

The e-commerce roadmap consists of 8 key areas, namely funding, taxation, customer protection, education and human resources, telecommunication infrastructure, logistics, cybersecurity, and establishment of a coordinating function (in the form of a steering and management committee). The following are several examples of key programs stipulated under the e-commerce roadmap.

(a) Taxation

With regard to tax, the Government plans to undertake 3 programs, namely (i) streamlining of tax obligation; (ii) drafting the procedure and guidelines for registration of e-commerce business; and (iii) promoting equal tax treatment for foreign e-commerce businesses.

(b) Customer protection

There are 3 programs related to customer protection: (i) drafting government regulation on e-commerce transactions; (ii) building customer trust; and (iii) using national payment gateway for e-commerce transactions in Indonesia.

(c) Logistics

Considering the rapid development of e-commerce business in Indonesia, the demands for logistics companies to deliver the goods from merchant to customer have also increased. As such, the Government wishes to increase the number of logistics service providers to ensure timely delivery across the country.

(d) Cybersecurity

According to the E-Commerce Road Map, under the purview of cybersecurity, the Government wishes to develop a national supervision system for e-commerce transactions in order for all e-commerce transactions in Indonesia to be monitored by the Government through an integrated electronic system. Aside from the obligation of all e-commerce companies to fulfil the requirements to support the system which is expected to be completed in January 2018, there is no further elaboration yet on what the national supervision system entails.

New Broadcasting Law in the Pipeline

The new draft broadcasting law continues to be discussed and debated both within the spectrum of the Indonesian parliament and also amongst stakeholders alike. After the most recent version of the draft broadcasting law proposed by the legislative body of the Indonesian parliament was rejected, one of the key issues currently debated back and forth with regard to digital broadcasting is on whether to apply a single multiplexer or a multiple multiplexer system.

In a single multiplexer scheme, basically the spectrum frequency intended for digital broadcasting will only be allocated to one entity, whereas in a multiple multiplexer scheme there will be more than one entity that will receive spectrum frequency allocation for digital broadcasting. The argument against the single multiplexer scheme is that the Government will have an overly dominant position to determine which broadcast will be transmitted, whereas those against the multiple multiplexer scheme assert that the Government should maintain ownership over the spectrum frequency as opposed to distributing them between a few private broadcasters.

App-Based Transportation Regulation Revised Yet Again

The issue of app-based transportation is proving to be controversial as the most recent regulation governing key players such as Go-Jek, Grab, and Uber that was issued earlier in 2017 was declared to be inconsistent with higher laws by the Indonesian Supreme Court. In response, the Indonesian government recently issued Ministry of Transportation Regulation No. PM 108 of 2017 on the Organization of Non-Fixed-Route Public Transportation Services ("**PM 108/2017**").

The new regulation introduces a number of novel provisions to be in accordance with the Indonesian Supreme Court decision which annulled the previous regulation, such as:

(a) Introducing government intervention to determine the operational areas of app-based transportation drivers;
(b) The Registration of Vehicle Registration Certificate used by an app-based transportation driver now may be made on behalf of the app-based transportation driver instead of previously being required to be on behalf of the app-based transportation provider;
(c) Revoking a number of prohibitions, such as those relating to: (i) determining tariffs and offering tariff promotions below the established base tariff, (ii) recruiting drivers, and (iii) providing app-based service access to individuals working as transportation providers and public transportation companies which have not yet secured non-fixed-route transportation licenses.

In addition, the new regulation also further defines the separation of tariffs for conventional taxis and app-based transportation providers, giving legal certainty on how conventional taxis and app-based transportation providers shall determine their tariffs within a cooperation between the two. Under PM 108/2017, conventional taxis tariffs shall be set in accordance with the use of taxi meters and base/ceiling tariffs as have been determined, whereas for taxi services which are arranged via an online application, payment should be based on tariffs which are set through the online application, and not through the use of taxi meters.

THAILAND

The Payment System Act will Take Effect in the Second Quarter of 2018

The Payment System Act B.E. 2560 (2017) ("**PSA**") was published in the government gazette on 18 October 2017 and will become effective 180 days thereafter (i.e. 16 April 2018). The PSA consolidates and reforms existing payment laws to bring them in line with international standards of governance. The PSA classifies e-payment related businesses into three categories: (a) important payment systems; (b) regulated payment systems; and (c) regulated payment services.

Under the PSA, existing operators of businesses falling within the category of regulated payment systems or regulated payment services are required to submit an application for a new license or reqistration within 120 days,

i.e. from 16 April 2018 to 13 August 2018. If such an application is not submitted within the prescribed period, the licensee will be prohibited from continuing the business. For some new businesses, such as those utilizing new financial technology and who are undergoing the trial stage or are provided to a limited number of customers without any impact on the payment system or public benefit on a broad scale, only registration is required. Only a limited company, a public limited company or other juristic persons as prescribed by the Bank of Thailand is eligible to register or apply for a license.

The Bank of Thailand is the key regulator under the PSA having the authority to announce rules and regulations for this new regulatory framework essentially concerning risk and security management, supervision over the financial status of operators, good governance, protection of customers and fostering competition on a level playing field.

FinTech Legislation has Undergone Public Hearings

The draft Act on Business Promotion and Public Access to Services through Financial Technology ("**FinTech Act**") is intended to create opportunities for established and potential business operators to maximize the use of FinTech in developing financial and investment services with less legal limitations and more efficient information access.

The draft FinTech Act contains four core matters: (a) strengthening the confidence in the execution of some types of electronic transactions which would be deemed as fully legitimate as normal transactions, (b) facilitating businesses' access to necessary information under possession of governmental agencies for the benefit of due diligence and know-your-client assessments, (c) supporting electronic non-face-to-face identity verification, and (d) allowing businesses to access anonymized data under possession of governmental agencies for the development of financial products and services, and supporting voluntary disclosure of anonymized data by the public and private sectors.

The draft FinTech Act has undergone public hearings and has been submitted to the President of the National Legislative Assembly.

Affordable Internet Access for Rural Areas: the Digital Transformation of the Country under the Thailand 4.0 Vision

Thailand 4.0 is the government's flagship policy which aims to transform Thailand into a digital economy with high value-added products and services. As part of the drive towards the innovative era, the government will increase high-speed internet access to people residing in rural areas by providing high-speed internet access at affordable prices and free Wi-Fi hot spots to support future industries, innovation and e-commerce. Such national broadband network under the Pracha Rat Internet project is planned to be rolled out across 24,700 villages by the end of 2017 and 72,000 villages within 2018.

VIETNAM

New Law on Technology Transfer

On 19 June 2017, the new Law on Technology Transfer was passed ("**New Law**"), which will supersede the existing Law on Technology Transfer (2006) ("**Old Law**") from 1 July 2018. The New Law sets out significant changes regarding the following issues:

(a) The New Law was passed for the purpose of increasing the country's productive capacity and competitiveness in both domestic and foreign markets. Compared to the Old Law which prescribed optional registration of technology transfer agreements, the New Law now requires certain technology transfer agreements to be registered with the science and technology authorities. These include cross-border technology transfers (whether to or from Vietnam) and domestic transfers that use state capital or funds from the state budget.
(b) For the purpose of limiting the transfer of outdated technologies and equipment into Vietnam, the New Law adds a separate chapter on appraisal of technologies used in investment projects.
(c) Instead of voluntary registration to obtain government incentives as provided by the Old Law, the New Law provides that most technology transfer agreements, except for independent technology transfer agreements and the licence of restricted transfer technology, are required to be registered with the competent authorities.[1]
(d) The New Law further specifies tax incentives that may be applied to certain entities, notably for incubators for science and technology (including for innovative start-ups).

New Regulation on Regulating the Conditions of Doing Business in Camouflaged Sound Recording, Video Recording and Positioning Devices and Software

On 19 May 2017, the Government issued Decree No. 66/2017/ND-CP on regulating the conditions of doing business in camouflage equipment and software used for audio and video recording and GPS ("**Decree 66**"). Decree 66 takes effect on 05 July 2017.

Accordingly, only the following business establishments are permitted to use camouflaged devices in their businesses:[2]

(a) Business establishments of the Ministry of Public Security that are granted certificates of satisfaction of security and order conditions by a competent agency of the Ministry of Public Security;
(b) Business establishments of the Ministry of National Defense that are granted certificates of satisfaction of security and order conditions by a competent agency of the Ministry of National Defense; and
(c) Business establishments other than those specified above that are granted certificates of satisfaction of security and order conditions by a competent agency of the Ministry of Public Security.

In addition, only the following business establishments may sell camouflaged devices to subjects permitted by law to secretly use sound recording and video recording measures:[3]

(a) Specialized agencies in charge of protection of national security and social order and safety; and

(b) Agencies responsible for executing secret sound recording and video recording measures under the conditions, competence and procedures for special procedural investigation measures prescribed by the Criminal Procedure Code.

[1] The New Law, Article 31.1
[2] Decree 66, Article 6.2
[3] Decree 66, Article 11.5

Technology, Media, And Telecommunications

Online System for Issuance of Work Permits

On 15 August 2017, the Ministry of Labour, Invalids and Social Affairs issued Circular No. 23/2017/TT-BLDTBXH to guide the online issuance of work permits to foreign workers in Vietnam. This circular will come into effect on 2 October 2017.

Under this circular, the labour authorities have implemented an online system through which work permits may be processed. Particularly, if electing to use the online system, the work permit procedures are as follows:

(a) At least 7 working days before the planned date on which foreign workers start working for the employer, the employer must electronically submit the declaration and application for work permit to the labour authorities through the designated website.
(b) Within 5 working days from the receipt of a sufficient declaration and application for the work permit, the labour authorities will respond to the employer by email to confirm the application. If the application is sufficient, the employer will, in person or by post, submit the original work permit application to the labour authority for verification and retention.
(c) No later than 8 working hours from the receipt of the original work permit application, the labour authority will issue its result to the employer in person or by post at the employer's election.

However, note that while the application procedure has been streamlined, the circular does not change the type of supporting documents required for the work permit. Therefore, employers/employees are still required to prepare the required supporting documents in accordance with the law.

Supplementation to Registration of Provision of Information Content Services

On 23 June 2017, Circular 08/2017/TT-BTTTT ("**Circular 08**") was promulgated by the Ministry of Information and Communications to amend Circular 17/2016/TT-BTTTT stipulating procedures for registration of provision of information content services on mobile telecommunication networks. This Circular 08 took effect on 21 September 2017.

According to Circular 08, mobile network operators ("**MNOs**") providing periodic services to subscribers have the following obligations:

(a) For subscribers who subscribe to periodic services, MNOs must send text messages to users notifying the automatic extension of the service with the following contents: name, code, number of the service, fee period, fee, cancellation method, customer care hotline. Such notice will be sent every 7 days for daily and weekly services, and every 30 days for monthly and yearly services, and must be sent between 7.00am and 10.00pm.
(b) For subscribers who cancel the services, MNOs must notify the result of such request via text message.[4]

Tightening the Management of Mobile Subscribers to Block Spam Messages

In an effort to prevent spam messages, the Government issued Decree No. 49/2017/ND-CP ("**Decree 49**") on the amendment of a number of regulations on management of mobile subscribers. This Decree took effect on 24 April 2017. Some notable points of Decree 49 are as follows:

[4] Circular 08, Article 1.3(b)

(a) The provision of Subscriber Identity Module ("**SIM**") cards to users shall only be conducted at Points of Telecommunications Services ("**PTS**") established by telecommunications companies or at PTS authorized by telecommunications companies.[5]

(b) Telecommunication companies are required to take and retain photos of persons directly entering into telecommunications services contracts.[6]

(c) Decree 49 abolishes the limit on the number of prepaid mobile subscriptions that each individual can register with each telecommunications company. However, from the fourth subscription, the user is required to conclude a contract with the telecommunications company in question.[7]

(d) Decree 49 also increases the administrative fine applicable to violations of the provisions thereof, with monetary fines increased up to VND 200 million.[8]

CAMBODIA

Sub-Decree on Fee Determination of Usage of Telephone Number and Telecommunications Numbers

The Royal Government of Cambodia has issued Sub-Decree No. 149 dated 05 September 2017 on Fee Determination of Usage of Telephone Numbers and Telecommunications Numbers ("**Sub-Decree No. 149**"). One mobile telephone number whether active or inactive costs USD 0.05 per annum in 2017/2018, USD 0.06 per annum in 2019/2020 and USD 0.08 per annum in 2021. One thousand fixed numbers held by an operator costs USD 0.05 per annum in 2017 and 2018, USD 0.06 per annum in 2019 and 2020 and USD 0.08 per annum in 2021. These costs shall be paid by the telecommunication operators every month to the Ministry of Posts and Telecommunications of Cambodia ("**MPTC**"). In addition, the telecommunication operators shall also pay a short code of USD 1,000 per annum to the Telecommunication Regulator of Cambodia. The Sub-Decree No. 149 entered into force on July 2017.

Sub-Decree on Authorisation for Operation in Sector of Information, Communication Technologies

The Royal Government of Cambodia has promulgated Sub-Decree No. 110 dated 21 July 2017 on Authorisation for Operations in the sector of Information, Communication Technologies ("**ICT**") ("**Sub-Decree No. 110**"). The Sub-Decree No. 110 is effective from the signatory date. Nevertheless, Article 36 of the Sub-Decree No. 110 provides one year of grace period to any person operating in the ICT sector to comply with the aforementioned Sub-Decree, including filing for an authorisation for operation at the General Department of ICT or Local Office of Post and Telecommunications.

To date, any person wishing to operate in the ICT sector shall have an authorisation from MPTC. Based on the type of business, Sub-Decree No. 110 regulates three types of authorisations, namely (a) Approval, (b) Certificate, and (c) License.

[5] Decree 49, Article 1(15.1)
[6] Decree 49, Article 1(15.5)
[7] Decree 49, Article 1(15.7)
[8] Decree 49, Article 2(30.8)

Sub-Decrees on Universal Service Obligation ("USO") and on Capacity Building, Researches and Development ("CBRD")

In implementing the Law on Telecommunications dated 17 December 2015 ("**Law on Telecoms**"), the Royal Government of Cambodia has promulgated two sub-decrees: (a) Sub-Decree No. 111 dated 21 July 2017 on Determination of System for Implementation of Programs of Universal Service Obligation in Telecommunication Sector ("**Sub-Decree No. 111**") and (b) Sub-Decree No. 112 dated 21 July 2017 on Determination of System for Management of Programs of Capacity Building, Researches and Development in ICT Sector ("**Sub-Decree No. 112**").

Important notes from Sub-Decree No. 111 are as below:

(a) USO funds are under management of the Council of the USO funds headed by the Minister of MPTC with participation of six colleagues from MPTC, National Institute of Posts, Telecommunications and ICT and Ministry of Economy and Finances. The Council of USO funds is assisted by a secretariat;
(b) Telecommunication operators can request, prior to the contribution into USO funds, to offset up to 50% of their contribution per annum with the implementation project of USO programs by complying with requirements stated in Sub-Decree No. 111. Any telecommunication operator which fails to request for offsetting prior to the contribution into USO can request for the offsetting only for the pending USO implementation project in 2017 and 2018 or for the USO implementation project achieved in 2017 or 2018;
(c) Telecommunication operators shall pay their first annual contribution of 2% of gross revenue on 2017.

Important notes from Sub-Decree No. 112 are as below:

(a) CBRD funds are under management of the Council of CBRD funds headed by the MPTC with participation of six colleagues from MPTC, Ministry of Economy and Finances, Ministry of Education, Youth and Sport and Ministry of Labour and Vocational Training;
(b) Telecommunication operators can request, prior to the contribution into CBRD funds, to offset up to 20% of their contribution per annum with the implementation project of CBRD. Unlike the USO funds, any telecommunication operator which fails to request for offsetting prior to the contribution into CBRD funds cannot request for offsetting with any pending or implementation project achieved;
(c) Telecommunication operators shall pay their first annual contribution of 1% of gross revenue on 2017.

Prakas on Connection and Transfer of Data of Telecommunications and Information Technology Service

The MPTC has issued Prakas No. 133 dated 27 April 2017 on Connection and Transfer of Data of Telecommunications and Information Technologies Service from Telecommunication Operators and Related Persons in Sector of Telecommunications to Management Centre of Telecommunications and Information Technologies ("**DMC**") ("**Prakas No. 133**"). Prakas No. 133 requires the telecommunication operators and related persons in telecommunication sector to connect with direct link to DMC so that the service data should be automatically transferred to and from the operators and related persons in telecommunication sector to DMC.

Prakas on Conditions and Legal Procedure of Granting, Modification, Suspension, Transfer and Withdrawal of Permit, Certificate or License on Telecommunication Operations

In implementing the Law on Telecoms, MPTC has issued Prakas No. 122 dated 07 April 2017 on Conditions and Legal Procedure of Granting, Modification, Suspension, Transfer and Withdrawal of Permit, Certificate or License

on Telecommunication Operations ("**Prakas No. 122**"). As prescribed in Article 15, Article 16 and Article 17 of Law on Telecoms respectively:

(a) Permit is granted for (i) importation, exportation, supply and distribution of telecommunication equipment, (ii) Internet service shop, (iii) sale and/or reparation of telecommunication equipment, (iv) publishing of telecommunication number directory and (v) other operations prescribed by Prakas of MPTC;
(b) Certificate is granted for (i) accreditation of qualified agent for importation, supply and distribution of telecommunication equipment, (ii) type approval of telecommunication equipment and (c) other operations prescribed by Prakas of MPTC;
(c) License is granted for (i) construction and/or provisioning services of telecommunication infrastructure and network and telecommunication supporting infrastructure, (ii) provision of telecommunication services and (iii) other operations prescribed by Prakas of MPTC.

Under the new regime, the telecommunication operation license is divided into three categories being (a) License on Infrastructure and Services, (b) License on Limited Infrastructure and Services, and (c) License on Telecommunication Services. The services being subject to these licenses are listed in the Schedule 5 of Prakas No. 122.

Under Article 15 of Prakas No. 122, the Permit or Certificate is valid for one year except for the Certificate of Type Approval of telecommunication equipment and communication radio equipment which is valid in perpetuity. The License on Infrastructure and Services and/or License on Limited Infrastructure and Services are valid for 30 years. The License on Telecommunication Services is valid for 15 years.

According to Article 34 (d) of Prakas No. 122, any holder of Permit, Certificate or License under the former regime shall request for exchange of Permit, Certificate or License within 180 working days from the publishing of the application form for Permit, Certificate or License under the new regime; otherwise, the Permit, Certificate or License under the former regime will be automatically repealed.

THE PHILIPPINES

Establishment of the Free Internet Access Program in Public Places

On August 3, 2017, Philippine President Rodrigo Duterte signed Republic Act No. 10929, otherwise known as the *Free Internet Access in Public Places Act* ("**RA 10929**") into law. Under this law, free internet service shall be provided in national and local government offices, public basic educational institutions, state universities and colleges, public hospitals and health centers, public parks, airports, seaports, transport terminals, and other public places. The law seeks to enable access to education, health, employment opportunities, and online government services for all Filipinos, especially those living in the countryside, who have limited or no access to the internet, and to promote knowledge-building among Filipinos, enabling them to participate and compete in the information and communication age. The Department of Information and Communications Technology ("**DICT**") shall be the lead agency to oversee the effective and efficient implementation of the law. In pursuance of this mandate, the DICT held its first public consultation for the proposed Implementing Rules and Regulations of RA 10929 on October 24, 2017.

Technology, Media, And Telecommunications

DICT Promotes the Adoption of ASEAN ICT Masterplan 2020

The DICT is promoting the adoption of the ASEAN ICT Masterplan 2020 ("**AIM 2020**") which envisions a highly evolved industry and ICT usage in ASEAN. AIM 2020 has eight (8) strategic thrusts: (a) Economic Development and Transformation, (b) People Integration and Empowerment through ICT, (c) Innovation, (d) ICT Infrastructure Development, (e) Human Capital Development, (f) ICT in the Single Market, (g) New Media and Content, and (h) Information Security and Assurance. Taking the lead and an active role in the pursuit of AIM 2020, the DICT "*sets the country's direction towards ASEAN economic integration, reaping the economic rewards brought about by ICT-enabled services.*" The end goal of these initiatives is a digitally-enabled economy that is secure, sustainable, and transformative, as well as an innovative, inclusive, and integrated ASEAN community.

DICT Releases the Framework for Digital Terrestrial Television Broadcasting Migration Plan

The DICT has released the Framework for the Digital Terrestrial Television Broadcasting Migration Plan which enjoins broadcasters, manufacturers, content producers, and end users, in a comprehensive nationwide implementation strategy for the expedient migration from analog to digital broadcasting come the Analog Switch Off ("**ASO**") target at the end of 2023. It is envisioned that the migration will contribute to growth in Philippines' broadcasting and related industries.

Data Breaches Sustained by the Bank of the Philippine Islands and COL Financial Group, Inc.

Following a recent incident which caused the temporary suspension of thousands of its clients' accounts, the Bank of the Philippine Islands ("**BPI**"), one of the largest and most prominent banks in the Philippines, was recently subjected to a privacy compliance check conducted by the National Privacy Commission ("**NPC**"), the regulatory and quasi-judicial body mandated to uphold the right to data privacy and ensure the free flow of information. The compliance check will evaluate BPI's compliance with the Data Privacy Act and seek to address gaps, especially in BPI's breach management protocol.

In another incident, COL Financial Group, Inc., a leading online stockbroker in the Philippines, notified the NPC of a possible data breach to its system. According to the company, it detected a "*possible breach*" in its system that "*may involve some personal client information.*" The NPC has assured the public that it is monitoring the COL Financial Group, Inc. and shall issue new information to all stakeholders as soon as available.

Recognizing the high-risk processing involved in their operations and to hopefully avoid any similar incident in the future, the NPC, in cooperation with the Bangko Sentral ng Pilipinas and the Bankers Association of the Philippines, recently conducted a general assembly of all the data protection officers from the Philippine banking industry.

Registration of Data Protection Officers and Personal Data Processing Systems

September 11, 2017 was the last day for the registration of registration of data protection officers ("**Phase 1 Registration**") with the NPC. Covered persons were required under the Data Privacy Act ("**DPA**") and its implementing rules and regulations ("**DPA IRR**") to register their respective data protection officers ("**DPOs**") with the NPC. Although late registration of the Phase 1 Registration is still ongoing, those who have failed to register their respective DPOs on time face compliance checks and orders from the NPC.

On the other hand, registration of personal data processing systems ("**Phase 2 Registration**") will be from January 2018 to March 8, 2018. Under the DPA IRR, a "data processing system" is defined as "*a structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing*".

PEOPLE'S REPUBLIC OF CHINA

Skype Removed from App Stores in China

Skype, the Microsoft-owned messaging and calling service provider, became the latest application to fall victim to the Chinese "Great Firewall", as reports emerged on 22 November 2017 that the Skype app had been removed from app stores in China. Skype joins Facebook, Google, Twitter, and Netflix on the long list of foreign technology companies that are not permitted to operate in China, as the Chinese government continues to strongly assert its doctrine of "cyber sovereignty", which the PRC government has recently codified into law, under which each country has the full right to govern the operation and use of the Internet within its borders. According to an Apple spokesperson, the removal of Skype from the Apple app store was due to a notification issued by the PRC Ministry of Public Security that Skype, along with a number of other VOIP apps, had failed to comply with certain local laws. This episode highlights the continuing struggle that foreign technology companies currently face, and will likely continue to face, in gaining access to the massive Chinese consumer market.

China Issues 3-year Plan Targeting Growth in Artificial Intelligence

On 18 December 2017, the PRC Ministry of Industry and Information Technology ("**MIIT**") released its action plan focused on driving the growth and development of the artificial intelligence ("**AI**") sector in China over the next three years. The action plan, which follows a similar vein to the strategic plan issued by the PRC State Council in September 2017, sets out key targets for research breakthroughs in AI to be achieved by 2020, with the developments in AI to be integrated across numerous other industries on a large-scale basis, including the areas of autonomous intelligent vehicles, AI-supported medical diagnosis, as well as facial and speech recognition. In view of the above goals, the action plan further sets the policy support that the MIIT intends to provide to the artificial intelligence industry, such as the allocation of a special pool of funds towards AI development, state support in talent cultivation and adopting of policies and regulations that provide a better business environment for AI companies.

The MIIT's action plan is likely to further stimulate competition in an already highly competitive sector in China. China's biggest technology companies (namely Baidu, Tencent, and Alibaba) are all already significantly involved in AI development and research, and there are a number of fast-growing Chinese AI companies (such as Face++ and SenseTime) that can give the bigger players a run for their money. To make things more interesting, Google, which is one of the biggest drivers in AI development globally, has also recently announced on 13 December 2017 its intention to establish a new AI research centre in Beijing.

Technology, Media, And Telecommunications

REST OF THE WORLD

AUSTRALIA

Notifiable Data Breaches ("NDB") Scheme Enacted

The NDB Scheme will take effect from 22 February 2018, and imposes an obligation to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm, referred to as an "eligible data breach". The notification must include recommendations about the steps individuals should take in response to the breach. The Australian Information Commissioner must also be notified of eligible data breaches.

The NDB scheme applies to all agencies and organisations with existing personal information security obligations under the *Privacy Act 1988*. Agencies and organisations that suspect an eligible data breach may have occurred must undertake a reasonable and expeditious assessment to determine if the data breach is likely to result in serious harm to any individual affected.

EUROPEAN UNION

European Commission Publishes Guidelines to Tackle Illegal Content Online

The European Commission ("**EC**") has published a Communication containing guidelines for online platforms to proactively prevent, detect, and remove illegal content inciting hatred, violence and terrorism. Under the guidelines, online platforms are advised to appoint points of contact to cooperate more closely with competent national authorities, and also encouraged to use trusted "flaggers" (i.e. entities with expertise knowledge on what constitutes illegal content) and automatic detection technologies to speed up detection and rapidly remove illegal content. Online platforms are also expected to clearly explain their content policy to users, and encouraged to issue transparency reports detailing the number and types of notices received. Internet companies should also introduce safeguards to prevent the risk of over-removal. The EC will monitor the progress made by online platforms and assess whether further measures are required, including possible legislative measures, in May 2018.

EUIPO Publishes Report on the Online Sale of Counterfeit Goods through the Appropriation of Domain Names

The European Observatory on Infringements of Intellectual Property Rights has published a study on online business models that are used to infringe IP rights. The report on the first phase of the study, which was published in July 2017, examined the different online business models including, for example, models that share digital content online, such as linking, torrent and streaming. This report focuses on such businesses' use of lapsed domain names that were previously registered by famous people and organisations to host websites that offer counterfeit goods. The study identified approximately 28,000 online businesses involved in such activity, but concluded that these businesses are likely to be controlled by a few operators and the locations of most of the hosting providers are the Netherlands, Turkey and the United States.

Technology, Media, And Telecommunications

EU Regulation 2017/1953 on Promotion of Internet Connectivity in Local Communities Published in Official Journal

On 1 November 2017, Regulation 2017/1953 of the European Parliament and of the Council of 25 October 2017 amending Regulations 1316/2013 and 283/2014 was published in the Official Journal, to promote internet connectivity in local communities that is free of charge and without discriminatory conditions under the "WiFi4EU" brand. This will allow public authorities to apply for EU financial assistance to install local wireless access points to provide free internet connectivity in public spaces, provided that such public authority is able to finance the operating costs for a minimum of three years.

The EC estimates an overall budget of EUR 120,000,000 for this project, and to provide appropriate financing, the financial envelope for the implementation of the Connecting Europe Facility in the telecommunications sector will be increased by EUR 25,000,000, with a potential to be increased to EUR 50,000,000. Such budget will be allocated in a geographically balanced manner across the member states on a first come, first served basis.

HONG KONG

Hong Kong Bourse Relaxes Rules to Attract Technology Listings

On 15 December 2017, the Hong Kong Exchanges and Clearing announced that it would reform the listing rules for IPOs to permit the listing of companies that issue shares with different classes of voting powers, more commonly known as dual-class shares. The rule revision, which is expected to come into effect in the second half of 2018, is widely seen as an attempt by the Hong Kong bourse to attract listings by internet companies and other technology companies that commonly utilize the dual-class share model, particularly after a number of major Chinese technology companies had chosen to list on other exchanges after their dual-class share proposal had been rejected in Hong Kong. While the new rules would permit companies with dual-class shares structures to list on the Hong Kong exchange, such companies will be required to have a minimum expected market capitalization of at least HK$10 billion. These companies would also need to meet a higher revenue threshold of HK$1 billion in the financial year preceding their listing if their expected market capitalization is below HK$40 billion.

INDIA

TRAI Commits to Upholding Net Neutrality

In contrast to the position recently adopted by the Federal Communications Commission in the US, the Telecom Regulatory Authority of India ("**TRAI**") issued a set of recommendations on 28 November 2017 in favour of net neutrality, recommending that the licensing terms applicable to internet service providers be expanded to prevent any discriminatory treatment of data, including the blocking, slowing or offering preferential speeds or treatment to any online content. These recommendations had been highly anticipated following an extended period of consultations and lobbying by parties on both sides of the debate over 2 years. The TRAI's support of net neutrality will no doubt be received favourably by internet companies, particularly those that provide over-the-top services and/or content.

It should be noted that the TRAI's recommendations, while a clear statement of regulatory intent, will only gain the force of law once they have been translated into formal regulations by India's Department of Telecommunications,

which may ultimately choose not to adopt certain elements of the TRAI recommendations. The relevant regulations are expected to be released by the Department of Telecommunications in early 2018.

Alphabet to Leverage Light Beam Technology to Provide Internet Connectivity to Rural India

On 14 December 2017, Alphabet X, the research arm of the Alphabet group, announced that it would be working with the state government of Andhra Pradesh and a local network operator to use its newly developed light beam technology to provide high-speed wireless internet across the state of Andhra Pradesh. The relevant light beam technology, also known as Free Space Optical Communications ("**FSOC**"), uses beams of light to deliver high-speed, high-capacity connectivity over long distances, and will be particularly useful to the rural portions of the state, where the linking of mobile phone towers to a wired connection would be expensive and difficult.

The arrangement with Alphabet X is part of the Andhra Pradesh state government initiative to connect an additional 12 million Indian households to the internet by 2019, and the increased consumer market for online goods and service that this may potentially achieve within Andhra Pradesh and other rural parts of India may present a significant and exciting opportunity for internet companies operating in India.

UNITED KINGDOM

Data Protection Bill Tabled in Parliament

The UK's third generation of data protection law, the Data Protection Bill ("**DP Bill**"), was published on 14 September 2017 and is being reviewed by Parliament. By introducing the DP Bill, the UK Government aims to replace the Data Protection Act 1998 with a new law that provides a comprehensive and modern framework for data protection, with stronger sanctions for malpractice. The new law will set new standards for protecting general data, in accordance with the EU GDPR, grant individuals more control over use of their data, and provide new rights to move or delete personal data. By implementing strong data protection laws and appropriate safeguards, the UK Government aims to ensure that the UK is prepared for Brexit, and that businesses will be able to operate across international borders.

UNITED STATES

FCC Repeals Net Neutrality Regulations

On 14 December, the Federal Communications Commission ("**FCC**") voted to repeal the net neutrality regulations set in place during the Obama administration (the "**2015 Regulations**"). Net neutrality generally refers to network providers treating all sources of internet content equally as well as consumers' right to access content and services on the internet on a non-discriminatory basis. Previously in 2015, industry groups had brought a lawsuit challenging the 2015 Regulations. The 2015 Regulations were upheld by the US Court of Appeals for the DC Circuit. This time, it appears that several states may challenge the repeal of the 2015 Regulations. New York Attorney General Eric T. Schneiderman issued a statement on 14 December that he will lead a multistate lawsuit to stop the rollback of net neutrality. Attorney General Schneiderman is also investigating the fake comments, numbering around 2 million, submitted during the net neutrality comment process.

SEC Takes Action to Halt ICO Scam

The Cyber Unit of the US Securities and Exchange Commission ("**SEC**") has taken steps to stop an Initial Coin Offering ("**ICO**") scam that has earned up to US$15 million in tokens from investors. The scam involves PlexCorps' offering of PlexCoin, a cryptocurrency which PlexCorps promised would generate a profit of 1,354 percent for investors in fewer than 29 days, a promise which is false according to the SEC. The Cyber Unit has frozen the assets of PlexCorps, its founder and another partner in the venture and filed charges against them for non-compliance with provisions of US federal securities laws on anti-fraud and registration.

Conclusion

This wraps up our summaries of the various pertinent TMT issues that have arisen at the end of 2017 and start of 2018. The pace of developments in the TMT sphere intensified over 2017, and these developments cut across the fields of artificial intelligence, cybersecurity, communications, data protection, digital currency, e-commerce, and social media, among others. We are happy to have been able to provide this summary for you, and we hope that you have found this overview useful. 2018 promises to be another exciting year, particularly with the proposed Cybersecurity Bill and amendments to the PDPA in Singapore, as well as the rapid pace of developments in the other ASEAN jurisdictions. As such, do stay tuned for our next regional update on the important developments in the TMT sphere.

Contacts

Rajesh Sreenivasan
Head, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

D (65) 6232 0751
F (65) 6428 2204
rajesh@rajahtann.com

Steve Tan
Deputy Head, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

D (65) 6232 0786
F (65) 6428 2216
steve.tan@rajahtann.com

Lionel Tan
Partner
Rajah & Tann Singapore LLP

D (65) 6232 0752
F (65) 6428 2119
lionel.tan@rajahtann.com

Benjamin Cheong
Partner
Rajah & Tann Singapore LLP

D (65) 6232 0738
F (65) 6428 2233
benjamin.cheong@rajahtann.com

Tanya Tang
Partner (Chief Economic & Policy Advisor)
Rajah & Tann Singapore LLP

D (65) 6232 0298
F (65) 6225 0747
tanya.tang@rajahtann.com

Mary Thel T. Mundin
Partner
Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)

D (632) 894 0377
thel.mundin@cagatlaw.com

Kuok Yew Chen
Partner
Christopher & Lee Ong

D (603) 2267 2699
F (603) 2273 8310
yew.chen.kuok@christopherleeong.com

Deepak Pillai Chandrasekaran
Partner
Christopher & Lee Ong

D (603) 2267 2675
F (603) 2273 8310
deepak.pillai@christopherleeong.com

Yau Yee Ming
Partner
Christopher & Lee Ong

D (603) 2267 2669
F (603) 603 2273 8310
yee.ming.yau@christopherleeong.com

Intan Haryati Mohd Zulkifli
Partner
Christopher & Lee Ong

D (603) 2267 2674
F (603) 2273 8310
intan.haryati@christopherleeong.com

Eko Basyuni
Partner
Assegaf Hamzah & Partners

D (62) 21 2555 7802
F (62) 21 2555 7899
eko.basyuni@ahp.co.id

Zacky Zainal Husein
Partner
Assegaf Hamzah & Partners

D (62)21 2555 7800
F (62) 21 2555 7899

zacky.husein@ahp.co.id

Supawat Srirungruang
Partner
Rajah & Tann (Thailand) Limited

D (66) 2656 1991
F (66) 2656 0833
supawat.s@rajahtann.com

Saroj Jongsaritwang
Partner
Rajah & Tann (Thailand) Limited

D (66)2656 1991
F (66) 2656 0833

saroj.jongsaritwang@rajahtann.com

Heng Chhay
Managing Partner
R&T Sok & Heng Law Office

D (+855) 23 963 112/113
F (+855) 23 963 116
heng.chhay@rajahtann.com

Chester Toh
Director
Rajah & Tann NK Legal Myanmar Company Limited

D (+95) 9 7304 0763
F (+95) 1 9665 537
chester.toh@rajahtann.com

Chau Huy Quang
Managing Partner
Rajah & Tann LCT Lawyers

D (+84) 8 3821 2382
F (+84) 8 3520 8206

quang.chau@rajahtannlct.com

Vu Thi Que
Partner
Rajah & Tann LCT Lawyers

D (+84) 8 3821 2382
F (+84) 8 3520 8206

que.vu@rajahtannlct.com

Please feel free to also contact Knowledge and Risk Management at eOASIS@rajahtann.com

Our Regional Contacts

RAJAH & TANN | *Singapore*

Rajah & Tann Singapore LLP
T +65 6535 3600
F +65 6225 9630
sg.rajahtannasia.com

R&T SOK & HENG | *Cambodia*

R&T Sok & Heng Law Office
T +855 23 963 112 / 113
F +855 23 963 116
kh.rajahtannasia.com

RAJAH & TANN 立杰上海
SHANGHAI REPRESENTATIVE OFFICE | *China*

Rajah & Tann Singapore LLP
Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*
Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

RAJAH & TANN | *Lao PDR*

Rajah & Tann (Laos) Sole Co., Ltd.
T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*

Christopher & Lee Ong
T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

RAJAH & TANN NK LEGAL | *Myanmar*

Rajah & Tann NK Legal Myanmar Company Limited
T +95 9 73040763 / +95 1 657902 / +95 1 657903
F +95 1 9665537
mm.rajahtannasia.com

GATMAYTAN YAP PATACSIL
GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*

Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)
T +632 894 0377 to 79 / +632 894 4931 to 32 / +632 552 1977
F +632 552 1978
www.cagatlaw.com

RAJAH & TANN | *Thailand*

R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

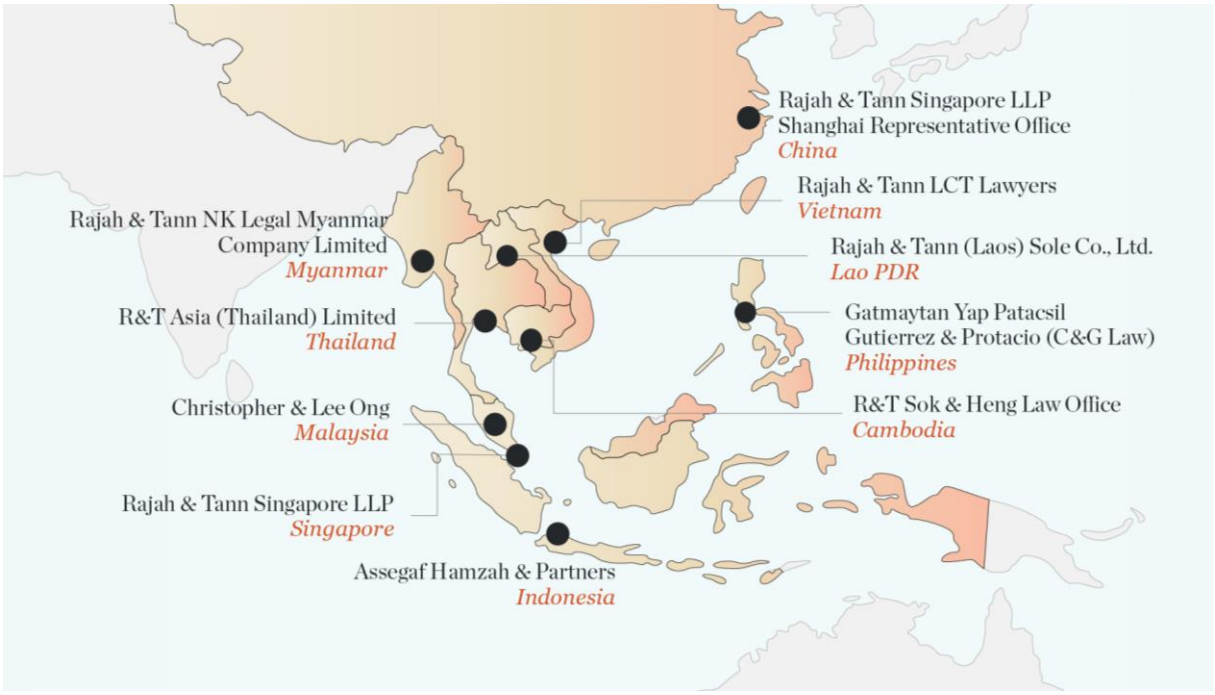
RAJAH & TANN LCT LAWYERS | *Vietnam*

Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 8 3821 2382 / +84 8 3821 2673
F +84 8 3520 8206

Hanoi Office
T +84 4 3267 6127
F +84 4 3267 6128
www.rajahtannlct.com

Our Regional Presence



Rajah & Tann Singapore LLP is one of the largest full service law firms in Singapore, providing high quality advice to an impressive list of clients. We place strong emphasis on promptness, accessibility and reliability in dealing with clients. At the same time, the firm strives towards a practical yet creative approach in dealing with business and commercial problems. As the Singapore member firm of the Lex Mundi Network, we are able to offer access to excellent legal expertise in more than 100 countries.

Rajah & Tann Singapore LLP is part of Rajah & Tann Asia, a network of local law firms in Singapore, Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Thailand and Vietnam. Our Asian network also includes regional desks focused on Japan and South Asia.