Technology, Media & Telecommunications

Technology, Media and Telecommunications Regional Update: A Recap from January 2018 to March 2018

Contents

Introduction

Welcome to the latest edition of our quarterly regional Technology, Media and Telecommunications ("**TMT**") update. The first quarter of 2018 has been a busy one, and we are excited to provide you short and easy-to-read write-ups on the latest developments in the ASEAN region.

As with our previous regional updates, these quick summaries have been prepared by our experienced TMT practitioners from the Rajah & Tann Asia network's members across ASEAN to share their views and thoughts on developments in the region. If you or your business partners wish to find out more about any of the updates here, please feel free to reach out to any of our regional offices in Rajah & Tann Asia.

RAJAH & TANN ASIA NETWORK

SINGAPORE

Select Committee on Deliberate Online Falsehoods – Causes, Consequences and Countermeasures

On 10 January 2018, the Singapore Parliament unanimously approved a motion for the appointment of a Select Committee to examine the issue of the deliberate perpetuation of online falsehoods and provide recommendations for measures to counter the spread of such falsehoods online. This motion targeting online falsehoods or "fake news" was moved by Law and Home Affairs Minister K. Shanmugam soon after a Green Paper on this matter was presented to Parliament on 5 January 2018. The Green Paper, titled "Deliberate Online Falsehoods: Challenges

and Implications", highlighted that tackling this issue was urgent in preparing Singapore, highly susceptible due to its openness and global connectedness, for the potential risks posed by such fake news. Such risks included the possibility of foreign players intentionally promulgating fake news online directed at undermining the credibility of public figures and institutions and causing rifts between Singapore's diverse racial and religious groups. We have detailed the Green Paper in our previous client update, which may be accessed here.

By the closing of submissions on 7 March 2018, the Select Committee had received 164 written submissions from individuals and organisations. The Select Committee held public hearings on 14 – 16, 22 – 23, and 27 – 29 March 2018. Over the course of the 8 days of public hearings, the Select Committee heard from 65 witnesses, including local and overseas experts, technology and media companies, community groups, civil society members, students, and other members of public. The Select Committee will work on a report when Parliament reconvenes in May.

PDPC Issues Response to Feedback Received from the Public Consultation Exercise on Proposed Revisions to the PDPA

On 1 February 2018, the Personal Data Protection Commission (the "**PDPC**") issued its response to feedback received from a public consultation ("**Public Consultation**") launched on 27 July 2017 on the review of the Personal Data Protection Act 2012 ("**PDPA**"). Having taken into account the feedback, the PDPC proposed the following amendments to the PDPA:

(a) providing two parallel bases for collecting, using, and disclosing personal data, namely, the Notification of Purpose basis for an organisation to collect, use and disclose personal data, and a proposed legitimate interests exception for organisations to collect, use or disclose personal data without consent. Organisations will be required to undertake a risk and impact assessment if seeking to rely on these alternative regimes; and

(b) refining the proposed mandatory data breach notification obligation. Having taken into account the responses provided, the PDPC has decided on retaining the criterion for mandatory reporting, namely, the breach must be of a significant scale before informing the breach to the PDPC. However, the PDPC removed the statutory threshold for the mandatory reporting.

We have detailed the Response in our previous client update, which may be accessed here.

Amendments to the Films Act Passed in Parliament

Amendments to the Films Act were passed in Parliament on 21 March 2018. The amendments to the Films Act are as follows:

(a) an automatic class licence scheme for retailers that sell video games on physical media. Under the licence scheme, retailers who repeatedly sell physical copies of age-restricted video games to underage buyers will be barred from selling such games, with the duration of such ban to be decided on a case-by-case basis;

(b) an optional co-classification scheme, which allows trained employees of some video companies to become film content assessors and classify films up to a PG 13 rating;

(c) expanded powers for IMDA officers to enter and search premises without warrant for serious offences, namely, those involving prohibited films and unlicensed public exhibition of films; and

(d) changes to the appeals process for films refused classification owing to national security concerns. The Minister for Communications and Information will now decide on the appeals, instead of the Films Appeal Committee.

Cybersecurity Bill Passed in Parliament

On 5 February 2018, Parliament passed the Cybersecurity Bill. Under the Cybersecurity Bill, owners of computer systems ("**Critical Information Infrastructure**") directly involved in the provision of essential services for national security, defence, foreign relations, economy, public health, public safety or public order will have to report cybersecurity incidents related to these systems, and comply with other statutory obligations, such as audit requirements, and participation in Cybersecurity exercises. We have detailed the Cybersecurity Bill in our previous client update, which may be accessed here.

Do note that while the Cybersecurity Act has been assented to by the President and has been published as Act Supplement 9 of 2018, it is not in force yet as there has not been any commencement notification.

GST on Digital Services by 2020

The Minister for Finance, Heng Swee Keat, has stated in his budget speech of 19 February 2018 that goods and services tax ("**GST**") will be imposed on imported digital services such as movie and music streaming services and mobile apps with effect from 1 January 2020. This tax will be introduced to ensure that imported and local services are accorded the same treatment.

Businesses selling imported services to consumers, such as media streaming platforms, will need to be GST-registered. Such businesses will include overseas vendors whose annual global turnover exceeds S$1 million, and whose sale of digital services to consumers in Singapore is more than S$100,000.

IMDA Consults on the Proposed Telecommunication and Subscription TV Mediation-Adjudication Scheme

The Info-communications Media Development Authority ("**IMDA**") has conducted a public consultation between 17 January 2018 to 28 February 2018 on the proposed Telecommunication and Subscription TV Mediation-Adjudication Scheme (the "**Scheme**"). The Scheme seeks to provide consumers access to an alternative platform for dispute resolution with their telecommunication and/or media service providers. The key proposed features of the Scheme includes the following:

(a) a two-stage mediation-adjudication process with mediation as the first phase, and adjudication as the second if necessary;

(b) adjudicated decisions will be final and binding only if the consumer accepts it;

(c) small business customers (businesses that employ 10 workers or fewer, register a revenue of S$ 1million or less in a year) and individuals who have a direct billing relationship with the service providers will be eligible for dispute resolution under the Scheme.

As of the date of writing, the IMDA has not yet issued its responses to feedback received on the proposed Scheme.

Technology, Media & Telecommunications

Additional funding for TeSA

The Minister for Finance, Heng Swee Keat, has stated in his budget speech of 19 February 2018 that the Government will set aside an additional S$145 million for the Tech Skills Accelerator ("**TeSA**"). He had stated in the speech that firms and people must develop digital capabilities as digital technologies continue to transform economies. TeSA will support more people to learn emerging digital skills such as in data analytics, artificial intelligence, the Internet of Things and cybersecurity.

Senior Minister of State for Communications and Information (the "**MCI"**), Dr. Janil Puthucheary, similarly states in his speech that TeSA will also target mid-career professionals for training, to ensure that they are prepared for disruptive changes in the economy.

Proposed Digital Government Blueprint

On 1 March 2018, the Smart Nation and Digital Government Office issued its press release titled, "Smart Nation on Track for Digital Transformation". In the press release, the Senior Minister of State for Communications and Information and Education, Dr. Janil Puthucheary, has stated that the Government intends to release a Digital Readiness Blueprint in the middle of 2018. The Blueprint will set out the Government's efforts in transforming itself to become more digital and data-driven. This will require the re-engineering of existing Government processes and digital infrastructure, such as the Government Technology Stack. For example, the revamped GovTech API Exchange had already been used in the MyInfo pilot, which allows banks to on-board new customers using Government-verified data.

Proposed National E-invoicing System

The Minister for Communications and Information, Assoc Prof Dr Yaacob Ibrahim**,** has stated in his Committee of Supply (Ministry of Communications and Information) speech of 6 March 2018 that as part of the SMEs Go Digital Programme, the Ministry of Communications and Information and Education is intending to accelerate sector digitalisation by putting in place common infrastructure that will raise business productivity. One such project is e-invoicing. The MCI hopes that such e-invoicing would assist businesses in cutting costs, ensure that companies are paid faster, and open up new financing options. The Minister has stated that the Ministry is currently studying this with various companies and will announce details of this project at a later date.

Development of an Innovation Cybersecurity Ecosystem

The Minister for Communications and Information, Assoc Prof Dr Yaacob Ibrahim**,** has stated in his Committee of Supply (Ministry of Communications and Information) speech of 6 March 2018 that the IMDA and the Cyber Security Agency of Singapore (the "**CSA**") are in collaboration with the National University of Singapore and Singtel Innov8, and that the aforesaid organisations are supporting the development of an Innovation Cybersecurity Ecosystem at Block 71. This initiative aims to help promising cybersecurity start-ups scale and internationalise.

The CSA will also introduce a Co-Innovation and Development Proof of Concept Funding Scheme which will support the development of cybersecurity solutions for critical infrastructure, national security, and classified system users.

Technology, Media & Telecommunications

Development of an OIP

The Minister for Communications and Information, Assoc Prof Dr Yaacob Ibrahim**,** has also stated in his Committee of Supply (Ministry of Communications and Information) speech of 6 March 2018 that the IMDA intends to scale Singapore-based Info-communications and Media ("**ICM**") companies. The IMDA currently runs the Accreditation@SG scheme, which seeks to scale Singapore-based ICM companies through deepening their capabilities. In line with the Accreditation@SG scheme, the IMDA intends to help build stronger ICM companies through piloting an "Open Innovation Platform" ("**OIP**"), which is a crowd-sourcing platform to facilitate collaboration between problem owners and a community of solution providers, to co-develop digital solutions that address business problems.

SAL Launches Future Law Innovation Programme, and Signs MOU with the IMDA and SMU

On 10 January 2018, the Singapore Academy of Law ("**SAL**"), launched its Future Law Innovation Programme ("**FLIP**"), a two-year pilot programme to encourage the adoption of technology, innovation, and the creation of a vibrant ecosystem for legal technology. The FLIP comprises three components:

(a) a Legal Innovation Lab located at the Collision 8 co-working Space;
(b) a virtual collaboration platform called LawNet Community; and
(c) South-East Asia's first legal tech accelerator to groom promising legal start-ups.

In assisting FLIP participants in technology adoption and innovation, the SAL is partnering the IMDA and the SMU. Memorandums of Understanding were signed between the parties on 10 January 2018. SMU will be SAL's academic partner in relation to legal innovation and the future business of law, co-host dialogues and seminars with the SAL, develop case studies and research on future law topics, and curate modular executive education programmes to support legal innovation for FLIP participants.

Technology, Media & Telecommunications

MALAYSIA

Anti-Fake News Bill Tabled in Malaysian House of Representatives

On 26 March 2018, the Anti-Fake News Bill (the "**Bill**") was tabled for its first reading in the Dewan Rakyat, or the Malaysian House of Representatives, after receiving Cabinet approval in the previous week.

The Bill was drawn based on the input of a special committee, which includes representatives from the police, the Attorney-General's Chambers, the National Security Council, the Malaysian Communications and Multimedia Commission (the "**MCMC**"), the Ministry of Communications and Multimedia, and the Department of Legal Affairs. Other stakeholders such as NGOs, lawyers, lecturers and politicians were also consulted.

The Bill is intended to "*deal with fake news and related matters*", whereby "fake news" has been broadly defined to include "*any news, information, data and reports, which is or are wholly or partly false, whether in the form of features, visuals or audio recordings or in any other form capable of suggesting words or ideas*".

Under the Bill, it is an offence to create, offer, publish, distribute, circulate or disseminate fake news, the penalty being a fine not exceeding RM500,000, imprisonment for up to 10 years, or both. Malaysian Courts are also empowered under the Bill to issue a court order for the offender to make an apology to persons affected by the fake news.

The Bill has extra-territorial application, applying to any person who spreads fake news if the fake news concerns Malaysia or if the person affected by the commission of the offence is a Malaysian citizen. Additionally, the Bill creates offences for providing financial assistance, whether directly or indirectly, to the spreading of fake news, as well as an offence for failure to remove any publication containing fake news. Every offence punishable under the new law is a seizable offence.

The introduction of the Bill has been met by heavy criticism by lawyers, politicians and the media alike, owing to the ambiguity in the definition of "fake news" and the potentially far-reaching implications of the proposed new law.

Existing laws which address fake news, such as the Communications and Multimedia Act 1998 will not be repealed. According to statements by the MCMC, the existing laws should be read together with the new law, and the new law is necessary to cater to current needs, as well as to address loopholes in existing laws

Section 233 of the Communications and Multimedia Act Held Constitutional by the High Court

After posting a doctored image of a magazine cover featuring the Prime Minister of Malaysia on his Facebook page in April 2016, a Malaysian Member of Parliament was charged with two counts of initiating and sharing two links of "*fake communication*" with the intention to offend others under section 233 of the Communications and Multimedia Act 1998 ("**CMA**").

Section 233(1)(a) of the CMA essentially prohibits publication of content deemed to be "*obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person*", any person found guilty of which would be liable, upon conviction, to a maximum fine of RM50,000 and/or a maximum one-year jail term.

Pursuant to these charges, an application was filed in the High Court of Malaya to challenge the constitutionality of Section 233 of the CMA on grounds that the section is "*too broad*" and is a violation of the rights enshrined in Article 10 of the Federal Constitution of Malaysia, which guarantees freedom of expression.

On 24 January 2018, the High Court of Malaya dismissed the application, ruling that CMA is constitutional and does not violate the Federal Constitution. In dismissing the application, the High Court judge ruled that freedom of expression is not absolute to those charged under section 233 of the CMA.

No Ban or Regulation on Cryptocurrency Trading at Present, but Traders are Still Subjected to Malaysian Tax Laws

In January 2018, the Second Finance Minister of Malaysia, on behalf of the Central Bank of Malaysia (Bank Negara Malaysia or "**BNM**") confirmed that BNM will not be enforcing a blanket ban on the trading of cryptocurrencies, as the Malaysian Government views digital currencies as part and parcel of Malaysia's "digitalisation roadmap" and a ban would curb innovation and creativity in the financial sector, particularly financial technology.

Notwithstanding that digital currencies are not currently regulated in Malaysia, the Inland Revenue Board of Malaysia ("**IRB**") has confirmed that cryptocurrency traders are still subjected to Malaysian tax laws. In imposing a freeze on the bank account of London based cryptocurrency exchanger Luno, the IRB stated that the freeze was to enable the IRB to determine whether the cryptocurrency company had complied with the requirements of the Income Tax Act 1967 ("**ITA**"), as cryptocurrency businesses are subjected to Malaysian income tax by virtue of the Section 3 of the ITA, which provides that tax shall be charged upon the income of any person accruing in or derived from Malaysia.

In a separate statement by IRB CEO Datuk Seri Sabin Samitah, the IRB has also confirmed that all property transactions in Malaysia using cryptocurrency will still be liable for real property gains tax (RPGT), as taxes should be paid even when property transactions are carried out with digital currencies.

Bank Negara Malaysia Issued Policy Document on Anti-Money Laundering and Counter Financing of Terrorism for Digital Currencies

On 27 February 2018, the BNM issued a policy document titled *Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Digital Currencies (Sector 6)* (the "**Policy Document**").

Digital currencies are not presently recognised as legal tender in Malaysia. Nonetheless, the Policy Document has been issued to ensure that effective measures are in place against money laundering and terrorism financing risks associated with the use of digital currencies and to increase the transparency of digital currency activities in Malaysia.

The Policy Document sets out, amongst others, the minimum requirements and standards that reporting institutions (i.e. any person offering services to exchange digital currencies) must observe when carrying out any one or a combination of the following types of activities:

(a) exchanging digital currency for money;
(b) exchanging money for digital currency; or
(c) exchanging one digital currency for another digital currency, whether in the course of carrying on a digital currency exchange business or otherwise.

BNM has highlighted that the reporting obligations imposed on the DCEs is the first step towards making digital currency activities more transparent in Malaysia, but it does not in any way connote the authorisation, licensing, endorsement or validation by BNM of any entities involved in the provision of digital currency exchange services

The MCMC and their Service Provider sued over Massive Data Breach Involving Personal Data of Millions of Malaysians

As reported in the previous TMT Regional Update, a massive scale data breach occurred in October 2017 whereby the personal data of millions of Malaysians were listed for sale on an online public forum by an unknown source, and regulatory authorities including the MCMC, the Personal Data Protection Commissioner's office ("**PDPC**") and Malaysian police force were investigating the breach.

In a twist of events, police investigations have traced the data breach to Nuemera (M) Sdn Bhd, i.e. the company engaged by MCMC to handle the Public Cellular Blocking Service ("**PCBS**") on behalf of MCMC. PCBS was launched by MCMC in 2014 to block lost or stolen mobile phones using its unique International Mobile Equipment Identity (IMEI) number.

Pursuant to these revelations, a civil suit has been filed against both MCMC and Nuemera by politician Fahmi Fadzil, who acts as the communications director for the People's Justice Party (Parti Keadilan Rakyat or "**PKR**").

The legal counsel for Fahmi Fazil have stated that the case will be based on breach of trust by MCMC for failing to guarantee the personal safety and personal information of the 46 million mobile subscribers. The leaked data included personal information such as individuals' names, mobile numbers, addresses and national identification numbers

Yet Another Massive Data Breach, Personal Details of More than 220,000 Malaysian Organ Donors and their Next-of-Kin Leaked Online

Following the massive-scale data breach involving 46 million Malaysian mobile phone users in October 2017, the online public chat forum, Lowyat.net reported in January 2018 that files containing personal details of more than 220,000 pledged organ donors had been leaked online as early as September 2016. The source of this latest leak has not been identified as of yet.

The recent data breach has far-reaching implications as it involves not only personal information of pledged organ donors, but also personal information of the nominated next-of-kin of the pledged organ donors. The presence of relationship information (e.g. spouse, sibling or parental) is said to increase the risk that victims of the data breach will be exposed to "social engineering" attacks, i.e. a form of manipulation to trick people into divulging confidential information by making use of the relationship information to gain the confidence of would-be victims.

In March 2018, Deputy Communications and Multimedia Minister Jailani Johari provided an update on the status of investigations into the two data breaches. According to the Minister, regulatory authorities including the MCMC, Department of Personal Data Protection ("**JPDP**"), the Attorney-General's Chambers of Malaysia, and the National Cyber Security Agency, were still investigating the matter under Section 4 of the Computer Crimes Act 1997 (which creates an offence for unauthorized access to computer material with intent to commit or facilitate commission of a further offence), and Section 130 of the Personal Data Protection Act 2010 (for the offence of unlawful collection of personal data).

Technology, Media & Telecommunications

Securities Commission Malaysia and the Central Bank of Malaysia caution Initial Coin Offering schemes

As at the date of this update, participation in Initial Coin Offering ("**ICO**") schemes (i.e. fundraising activities / investment schemes through the issuance and sale of digital tokens in exchange for investors paying for these tokens through cryptocurrencies) is neither prohibited nor regulated in Malaysia.

However, in early January 2018, the Securities Commission Malaysia ("**SC**") issued a cease and desist order to CopyCash Foundation (a Singapore-based blockchain startup) to immediately cease and desist all its proposed activities including a purported plan to launch an ICO in Malaysia, after the SC found that there was a reasonable likelihood that disclosures in CopyCash Foundation's white paper and representations to potential investors would contravene relevant requirements under Malaysian securities laws.

Following this event, the SC, together with the BNM issued a joint cautionary statement on ICO schemes in Malaysia, stressing that ICO schemes may involve activities that are subject to laws administered by the SC and BNM, and that carrying on such activities without proper authorisation will be an offence, whereby both authorities will not hesitate to take action against any offenders.

In the statement, issuers of ICOs are cautioned to be mindful that the launching of an ICO, the offering of digital tokens in exchange for digital currency or any form of payment and related activities, may trigger regulatory requirements under existing securities laws.

The SC and BNM also list the types of activities that ICO operators are prohibited from carrying out without the necessary approval or authorisation, and have further reminded members of the public to exercise caution before participating in any ICOs, including by first referring to the list of institutions that are licensed or approved to carry out regulated activities under the laws administered by the SC and BNM

Technology, Media & Telecommunications

INDONESIA

Introduction

In the first quarter of 2018, there has not been much development in the TMT sector as the year seems to be suffering from a slow start, both in the executive and legislative spheres – perhaps due to the upcoming general election in Indonesia next year.

Among the few developments are the completion of the registration of telecommunication service consumers, and the increasing demand for the Indonesian government to issue the Draft Government Regulation on E-Commerce following the issuance of the Indonesian e-commerce roadmap late last year.

While making no significant regulatory development on the technology space so far, the Minister of Communication and Information Technology ("**MOCIT**") has publicly announced that there are a number of draft regulations in the pipeline, including an elaboration on the e-commerce safe harbour policy which was introduced in 2016 and amendment to the legal framework on Internet negative content.

Finally, the recent Facebook-Cambridge Analytica data breach, involving the personal data of around 50 million Facebook users allegedly being used for the US President Donald Trump's presidential campaign, ignited concerns over unauthorized use of personal data world-wide, including Indonesia.

Personal Data Protection Concerns in the Mandatory Telecommunication Service Subscriber Registration

After first issuing the obligation in 2016, the Indonesian Government re-asserted that all telecommunication service consumers must register their information (personal information as contained in the Identity Card and Family Card) with their respective telecommunication service provider by 28 February 2018 or they will have their mobile number blocked. This is contained in the amendment regulations to Minister of Communication and Information Technology Regulation No. 12 of 2016 on Telecommunication Service Subscriber Registration.

However, even though the deadline has passed, a few issues have arisen regarding the mandated telecommunication service subscriber registration obligation - in particular, reports of leaks of the personal data of telecommunication service subscribers. A number of people have found that information on their Residential Identity Card and Family Card has been leaked and been used to register multiple mobile phone numbers.

In response, a civil claim is intended to be filed against the Indonesian government for damages caused by the personal data leak. The telecommunication service subscribers that were affected asserted that the Indonesian government must not turn a blind-eye to this issue and promptly provide a solution for those who were affected even though the deadline for the registration has passed.

Draft Government Regulation on E-Commerce

After the Indonesian government introduced the e-commerce roadmap and safe harbour policy for e-commerce platforms, it is expected that the Draft Government Regulation on E-Commerce will soon be enacted. Along with the Bill on Personal Data Protection, the Draft Government Regulation on E-Commerce will fill the current gaping hole in Indonesia's technology legal framework. According to findings of the Indonesian Consumer Institution Foundation ("**ICIF**"), most of the complaints it has received in 2017 were related to e-commerce cases, and ICIF argued that these cases were the result of lack of legal certainty and legal protection of the consumers.

Although Indonesia has an existing set of provisions on electronic transactions, there is much to be desired from the upcoming Draft Government Regulation on E-Commerce, such as right of withdrawal (i.e., the consumer's right to cancel any purchase) and online dispute resolution, as well as much needed clarification on the role of e-commerce platforms as intermediaries between buyers and sellers. It is expected that when the Draft Government Regulation on E-Commerce is enacted, it will bring betterment to the national e-commerce industry as a whole.

Government to Amend Regulation on Blocking of Negative Internet Content

Following the Indonesian government's decision to block Tumblr, MOCIT has been planning to revise its regulation on the blocking of negative Internet content, namely Minister of Communication and Information Technology Regulation No. 19 of 2014 on Control of Internet Websites Containing Negative Content.

An aspect that was recently discussed in the intended revision is to require internet service providers to provide space on the landing page when a consumer accesses a blocked website page for public services, specifically for public service announcements. This is following recent issues on several internet service providers exploiting the landing page upon accessing a blocked website page for commercial purposes (advertisements).

It is also hoped that the revision will also make the necessary changes to reflect what is stipulated under the amended Electronic Information and Transactions Law (No. 11 of 2008), namely Law No. 19 of 2016 on the Amendment to Law No. 11 of 2008 on Electronic Information and Transactions. The amended law empowers the Indonesian Government to block any access to or instruct the relevant electronic systems provider to block access to any negative content in the Internet.

It is expected that the revision will also incorporate provisions that will authorize the Indonesian government to use web crawlers and artificial intelligence to track down negative content on the Internet, after which the identified content will be reviewed by a dedicated team under MOCIT that will determine whether the website page will be blocked or not.

Safe Harbour Regulation to be Issued Together with Negative Content Control

In addition to the amendment to the regulation on blocking access to negative content on the Internet, MOCIT has expressly shown its interest in issuing a new regulation on safe harbour policy for e-commerce platforms.

The safe harbour policy was initially issued through Minister of Communication and Information Technology Circular Letter No. 5 of 2016 on the Limitations and Responsibilities of Platform Providers and Merchants in E-Commerce Using User-Generated Platforms, which prohibits certain types of content from being posted on user-generated content e-commerce platforms and defines the obligations and responsibilities of the parties involved in such platforms, and sets out a safe harbour policy to limit the scope of liability.

It is expected that these provisions will be incorporated and further elaborated into a new regulation to be issued by MOCIT and will also incorporate provisions related to negative content control. However, it is currently unclear whether this means that the amendment to Minister of Communication and Information Technology Regulation No. 19 of 2014 on Control of Internet Websites Containing Negative Content will be combined with this new regulation or these negative content control provisions will cover platforms other than website pages (such as apps and other third-party software).

Technology, Media & Telecommunications

Facebook-Cambridge Analytica Data Breach Re-sparks Personal Data Protection Concerns

After Facebook's personal data issue came to light, the concern for Indonesia's lack of a main legislation on personal data protection has rekindled, with experts noting the reluctance of Indonesia's legislative parliament to move along discussions on the Bill on Personal Data Protection, which was not included in this year's priority list. Despite this issue, MOCIT has reassured that they will continue pressuring the Indonesian legislative body to proceed with discussions on the Bill on Personal Data Protection.

The Facebook case also led MOCIT to assert that there will be consequences if Facebook, or any other social media, allows or encourages the unauthorized use of personal data of Indonesian nationals, while also stating that there will be severe criminal sanctions of up to 12 years of imprisonment and a fine of IDR 12 billion for those who fail to adhere to this warning.

In addition to criminal proceedings, MOCIT assures that the Indonesian government will not hesitate to block access to any social media that fails to respect the privacy rights of Indonesian nationals. Most recent notable blocks by the Indonesian government include Telegram and Tumblr, of which the blocking on the former has been lifted following Telegram's cooperation with MOCIT to handle any negative content on its platform.

Technology, Media & Telecommunications

VIETNAM

Implementing the Law on Access to Information

On 23 January 2018, the Government issued Decree No. 13/2018/ND-CP ("**Decree 13**") to provide details and execution methods of some articles in the Law on Access to Information. The main regulations mentioned in the Decree 13 are as follows:

(a) methods of facilitating the disabled and residents in border regions, islands, mountainous regions, areas facing extremely difficult social and economic conditions in exercising the right of access to information;
(b) the access to information of citizens via organizations, unions, enterprises;
(c) the forms for information requests;
(d) the responsibilities of the unit in charge of providing information.

This Decree shall take effect on 01 July 2018.

Decision on Promulgation of a Regulation on Cyber Information Security

On 12 February 2018, Ministry of Finance promulgated Decision No. 201/QD-BTC ("**Decision 201**") which outlines the legal framework of cyber information security and replaces Decision No.3317/QD-BTC dated 24 December 2014 issued by the Ministry of Finance. Decision 201 stipulates the Ministry of Finance's application of the Law on Information Security, related regulations, standards and measures. Under Decision 201, organisations in the finance sector are required to undertake protective measures when handling confidential information and information on the list of State secrets in accordance with State regulations and the Ministry of Finance's regulations on the protection of State secrets.

Amendments and Supplementation on the Management, Provision, and Use of Internet Services and Online Information

The Decree 27/2018/ND-CP ("**Decree 27**") issued on 1 March 2018 amendment to the Decree 72/2013/ND-CP dated July 15, 2013 on management, provision, and use of Internet services and online information, the Decree 27 provides amendments and supplementations of the remarkable provision. They are as follows:

(a) A news website or a social networking website must use at least one domain name ".vn" and store data in a server system, having IP address in Vietnam.

(b) Technical equipment system of social networking website must satisfy the following:

i Ensuring that there is at least one server system located in Vietnam for the purpose of inspection, storage, or post, at any time;

ii Storing information about accounts, time of login and log out, IP addresses of users and log of processed information for at least two years;

iii Receiving and processing users' reports of violations;

iv Detecting, warning, and blocking illegal access, online attacks, and meeting standards for ensuring information safety; and

v Having back up plans for maintaining safe and consecutive operation and resolving any problem which occurs, except for force majeure events.

(c) The Decree 27 also specifies procedures of issuance, amendments and supplementation, renewal, reissuance, and withdrawal of Certificate of Eligibility to open gaming centres.

The Decree takes effect on 15 April 2018.

New Regulation on Amendment of Fees for Telecommunications Operations and Charges for Issuance of License

On 12 January 2018, the Ministry of Finance issued Circular No 03/2018/TT-BTC ("**Circular 03**") on amendments to some articles of the Circular No 273/2016/TT-BTC, dated 14 November 2016 of the Ministry of Finance on fees for telecommunications operations and charges for issuance of license for telecommunication services and license for telecommunications operations and collection, waiver, transfer, management and use thereof.

Circular 03 provides amendments on fees for telecommunication services and fees for the establishment of a public telecommunication network. In addition, the schedule of fees and charges for issuance of a license for telecommunications operations have been amended accordingly (e.g. reducing the fee of repair and maintenance of submarine telecommunications cable lines (payment for each time of repair and maintenance of cable lines) from 500,000 US dollar to 50,000 US dollar).

This Circular was enforced on 1 March 2018.

Technology, Media & Telecommunications

CAMBODIA

Sub-Decree on Digital Signature

On 29 December 2017, the Royal Government of Cambodia issued a Sub-Decree No. 246 on Digital Signature ("**Sub-Decree No. 246**"). The Sub-Decree No. 246 aims to regulate and promote the usage of digital signature within the Kingdom of Cambodia in a highly secured and efficient way.

According to the Sub-Decree, the Ministry of Posts and Telecommunications of Cambodia ("**MPTC**") has the authority to monitor the digital signature and to issue the digital signature certificate to ministries and other public institutions, national and sub-national authorities.

The General Department of Information and Communication Technologies ("**GDICT**") assists the MPTC in the management of, issuance of, supervision and surveillance over the licence on digital signature certification ("**License**") for private entities who wish to become a digital signature certification authority ("**Certification Authority**").

The application for License must be submitted to the GDICT in accordance with the requirements set forth in the Sub-Decree No. 246 and related regulations. In addition, the applicant shall demonstrate respective technical skills, financial resources, business guarantee, ICT equipment, and other qualifications set forth by Prakas of MPTC. The License has a 10 years validity and can be renewed under the approval of the minister of MPTC.

Those who wish to obtain a digital signature certificate should submit a request to the Certification Authority. The Sub-Decree No. 246 mandates the use of digital signature for financial online operations, unless otherwise prescribed by inter-ministerial Prakas of the Ministry of Economy and Finance, MPTC and the National Bank of Cambodia to be in place separately.

Failing to obtain a License from MPTC in conducting the certification of digital signature will lead to a provisional fine of KHR 5,000,000 (approx. US$1,250) to KHR 15,000,000 (approx. US$3,750) for a natural person. A legal person will be fined KHR 50,000,000 (approx. U S$ 12,500) to KHR 150,000,000 (approx. US$ 37,500) for the same infringement.

Implementation of Programs of Universal Service Obligation in Telecommunication Sector and Capacity Building, Researches and Development in ICT Sector

On 6 February 2018, the MPTC held a press conference on the Universal Service Obligation ("**USO**") funds and Capacity Building, Researches and Development ("**CBRD**") funds to introduce key implementation measures as regards these funds.

The above introduction was part of the implementation of recent regulations governing USO and CBRD funds. To recall, these regulations include Sub-Decree No. 111 on Determination of System of Implementation of Programs of Universal Service Obligation in Telecommunication Sector ("**Sub-Decree No. 111**") and Sub-Decree No. 112 on Determination of System for Management of Programs of Capacity Building, Researches and Development in ICT Sector ("**Sub-Decree No. 112**").

According to these regulations, the telecommunication operators have to contribute 2% of their gross revenue per annum into USO funds and 1% of their gross revenue per annum into CBRD funds. The Sub-Decree No. 111 and

Sub-Decree No. 112 provide an avenue for telecommunication operators to request, prior to their contribution, offset of such contribution with the implementation project of USO and CBRN programs up to 50% and 20% respectively of their contribution per annum.

Under the USO, the funds are to be used for the objectives of narrowing down the digital divide by (i) construction and extension of telecommunication networks and infrastructures and of supporting telecommunication infrastructure for internet broadband toward the sub national authorities, rural and low income areas, public or free education institutions, public or free researches institutions, national, local and free libraries, public or free hospitals, or public or free health care centres; (ii) provision, strengthening and extension of modern and broadband telecommunication and ICT services in the aforementioned areas with security and safety; and (iii) provision of free emergency calls within Cambodia.

According to the press release, the secretariat of Council of the USO funds has been finalising the draft action plan for the implementation of the USO program for 2018. As the drafting process progresses, the Council of the USO funds has determined six areas of different social and economic conditions as priority areas for the implementation of the 2017's USO program. Those areas locate in Kamphong Chhnang, Kandal, Sihanouk Ville, and Koh Kong provinces. The working group of USO funds secretariat is currently measuring the service coverage in some areas, inclusive of the aforementioned priority areas, in order to invite the telecommunication operators who have fulfilled their contribution obligation regarding USO funds to check the service coverage in real time and eventually submit any project that can be qualified for offsetting their contribution obligation.

As for CBRD, the funds are to be used for (i) construction of infrastructures, innovation centres, laboratories, laboratories for the services of education, researches, development and innovation in sector of telecommunications and ICT ("**T-ICT**"); (ii) education and training in T-ICT majors, (iii) researches, development and innovation in T-ICT sector; (iv) supporting the business and new service creations in T-ICT; (v) provision of scholarship in T-ICT majors; (vi) supporting the events in development of human resources and promoting the researches, development and innovation in T-ICT sectors; and (vii) developing the competition events on modernisation of technologies and on best entrepreneurship in T-ICT sector.

As part of the implementation measures, the Council of CBRD funds has decided to use CRBD funds for three strategic objectives: (i) promotion of human resource development in ICT; (ii) promotion of researches, development and innovation in ICT; and (iii) promotion of new creations in ICT. As a result, the Council of CBRD funds has approved the (i) project of construction of innovation and entrepreneurship centre; (ii) offsetting of the implemented projects such as scholarships and training on entrepreneurship in ICT; and (iii) consideration of extension of computer training classes in high schools all over the country.

Digital Economy

It is observed that the MPTC has noticeably focused on expanding the understanding of digital economy in Cambodia to Cambodian citizens. On 6 February 2018, the MPTC held its first digital-economy workshop on "Start-up Policy Hack" as a platform whereby the participants and relevant partners could exchange ideas on the challenges posed by the digital ecosystem. The workshop was also used as a platform for the MPTC and those who were interested in formulating a policy to tackle a digital disruption through the creation of new approaches in the forms of openness, collaboration and practical-oriented solutions.

Additionally, on 06 March 2018, the MPTC pointed out its focus, during a meeting with the representatives from telephone manufacturers, on the creation of a platform where youth can demonstrate their skills in starting up their

business in the ICT sector. The MPTC also added that it has cooperated with the Ministry of Industry and Handicraft and other relevant ministries in encouraging and motivating start-up and SME businesses. According to the MPTC, the USO and CBRD funds also play significant role in developing the digital economy.

Technology, Media & Telecommunications

THE PHILIPPINES

DICT to Consider the HCLOS Formula in Determining the New Major Telecommunications Player

Last 27 February 2018, the Department of Information and Communications Technology ("**DICT**"), together with the National Telecommunications Commission, conducted the 2nd Stakeholders' Consultation on the Entry of a New Major Telecommunications Player. Among the suggestions for the criteria for selection was to use the Highest Committed Level of Service ("**HCLOS**") Formula. The HCLOS formula considers the number of services offered, speed, and the coverage percentage of cities up to the 6th class municipalities.

The Philippine Senate Unanimously Approves the Lifetime Cellphone Number Act

By a vote of 20-0, the Philippine Senate rendered its stamp of approval to Senate Bill No. 1636 or the Lifetime Cellphone Number Act. One of the salient features of the bill is mobile number portability whereby consumers are given freedom to choose their service providers without having to change their mobile numbers. In this connection, the current version of the bill likewise grants privacy of data over mobile numbers and other related personal information of consumers. The bill is currently pending in the House of Representatives.

The Philippine Senate Passes the National ID Law

Senate Bill No. 1738, otherwise known as the Philippine Identification System Act of 2018 (the "**Bill**"), was approved on its third and final reading before the Philippine Senate on 19 March 2018. The Bill aims to enforce a single official identification for all citizens and foreign residents in the country with each individual being issued a PhilSys Number, a randomly generated identification number, which shall be incorporated in all identification systems of government agencies. This number shall be found on the Phil ID itself, along with the full name, facial image, date of birth, address, and fingerprints of the bearer.

To protect a card bearer's right to privacy, Senator Panfilo Lacson, sponsor of the Bill, stated that the information under the Phil ID Registry shall be released only under the following conditions:

(a) Upon the consent of the registered person, specific to the purpose prior to the processing;

(b) Upon risk of public health and safety when relevant information may be disclosed, provided the risk of significant harm to the public is established and the owner of the information is notified within 72 hours of the fact of such disclosure;

(c) Upon order of the court; or

(d) When a registered person requests access to his or her registered information and record history, subject to the guidelines and regulations to be issued by the Philippine Statistics Authority.

Incidentally, since the House of Representatives has passed a similar bill, Presidential Spokesperson Harry Roque stated that "the next procedure is for the Senate and the House to reconcile their respective versions. After which it will be ratified by both Houses." It is thus expected that the Bill will be passed as law before the next adjournment of Congress in June 2018.

Technology, Media & Telecommunications

The Philippines National Privacy Commission Extends Deadline for Filing Annual Security Report

Originally set on 31 March 2018, the National Privacy Commission, the Philippines' data privacy agency, has announced that the deadline for covered organizations and professionals to file their respective annual security incident reports has been extended to 30 June 2018. The annual security incident report is among the yearly compliance obligations of Personal Information Controllers ("**PICs**") and Personal Information Processors ("**PIP**"), as provided in Philippine Data Privacy Laws.

Considering that this is the first time that PICs and PIPs will be submitting their annual security incident reports, the NPC has plans of releasing a version of the report that is more concise and easier to prepare, and in line with the requirements of other privacy regulations in the world, including the General Data Protection Regulation and the APEC Cross Border Privacy Rules

The Philippines to Draft Rules on Cryptocurrency Trading

The Philippines' Securities and Exchange Commission ("**SEC**") has stated that it is crafting rules to regulate cryptocurrency transactions to protect investors and reduce the risk of fraud. With initial coin offerings in the Philippines having started since 2017, Emilio Aquino, the SEC Commissioner in charge of enforcement and investor protection, has confirmed that the regulation, which will cover issuance and registration of cryptocurrencies, shall be finalized this year. Cryptocurrencies, a form of digital money that is created and maintained by users, has recently gained traction among investors and unfortunately, without proper regulation, some promoters of such currencies have scammed unknowing individuals.

NGCP and DICT Agree to Partner for the National Broadband Program

The DICT and the National Grid Corporation of the Philippines ("**NGCP**") shall soon sign an agreement to use NGCP's fiber optic capacity for the implementation of the National Broadband Program.

The NGCP said that it is willing to enter into a bilateral agreement with the government for the lease of its fiber optic network to make it available for use of third parties at no cost.

Technology, Media & Telecommunications

PEOPLE'S REPUBLIC OF CHINA

Anti-Unfair Competition Law Now Effective

China's revised Anti-Unfair Competition Law (the "**AUCL**") came into effect on 1 January 2018. Amongst other changes, the revised AUCL accords greater protection to unregistered (but well-known) trademarks by prohibiting the imitation of well-known identifiers of individuals or organisations, to prevent the relevant public from being confused. Protection afforded to trade secrets has also been expanded, as businesses are now prevented from using trade secrets illegally obtained by others. Finally, the revised AUCL also define certain online acts of businesses deemed as unfair, such as the inflation of online orders, and the fabrication of online reviews.

We have detailed the revised AUCL in our previous client update, which may be accessed here.

China Releases New Personal Information Privacy Standards

On 25 January 2018, China released the final version of the Information Technology - Personal Information Security Specification. While the Specification is a voluntary framework, the Specification sets out the best data protection practices that organisations in China should put in place. The Specification lays out general data protection standards such as the obtaining of consent before personal information may be collected and that information collected may only be used for purposes reasonably connected with the original purpose of such collection. Individuals are also accorded access and correction rights under the Specification, and the standards specified are similar to that under the European Union's General Data Protection Regulation.

REST OF THE WORLD

AUSTRALIA

New Notifiable Data Breach Scheme Sees a Considerable Number of Data Breach Notifications

Australia's mandatory data breach notification scheme, the Notifiable Data Breach ("**NDB**") Scheme came into force on 22 February 2018. Within less than 30 days of the Scheme coming into effect, there have been 31 data breaches notified in compliance with the NDB Scheme. One particularly serious data breach that has been notified under the NDB Scheme is a data breach suffered by Svitzer Australia which impacted about half of its Australian employees. This data breach involved an estimated 50,000 to 60,000 emails being auto-forwarded out of the company from the email accounts of 3 employees of the company, over a period of close to 11 months. The contents of these emails may have included employees' sensitive personal information such as their tax file numbers.

EUROPEAN UNION

Proposed e-Privacy Regulation

On 10 January 2017, the European Commission (the "**EC**") issued its proposal for a Regulation on Privacy and Electronic Communications (the "**Proposal**") to replace the current e-Privacy Directive. The Proposal will have a broader scope of application, as e-Privacy rules will be extended to new forms of electronic communication services such as machine-to-machine communications (the Internet of Things). Proposed amendments will also require that browser settings should disable cookies by default, to prevent other parties from storing information on the device, or processing information stored on the device without the user's consent. Finally, the Proposal also states that a valid "opt-in" consent must be obtained from the user in order to send unsolicited electronic communications such as e-mails, push notifications or SMSes.

EC's Fintech Action Plan

On 8 March 2018, the EC released a Fintech Action Plan (the "**Action Plan**"). The initiatives under the Action Plan may be classified under three broad categories:

(a) the Action Plan seeks to facilitate business growth, whilst protecting the interests of consumers and investors. For example, consistent licensing requirements will be imposed on fintech companies, crowdfunding service providers, and cypto-assets and initial coin offerings respectively, which will encourage the growth of these businesses whilst providing sufficient consumer / investor safeguards;

(b) the Action Plan seeks to support technological innovation in the Financial Sector. These initiatives may be sub-classified into 5 different categories.

i the EC is encouraging European Supervisory Authorities (the "**ESA)** to use innovation facilitators such as regulatory sandboxes to facilitate innovative businesses;

ii the EC also intends to remove obstacles to cloud services. For example, the EC is inviting ESAs to determine if guidelines on outsourcing to cloud service providers are needed. The EC is also encouraging stakeholders to establish their own regulatory codes of conduct;

iii the EC intends to carry out a blockchain initiative. The EC intends to assess how blockchain may be used as a digital services infrastructure, and how a comprehensive approach to blockchain and distributed ledger technology may be developed;

iv the hosting of an EU FinTech Lab; and

v the EC will evaluate how technology may aid consumers in comparing and finding suitable retail investment products.

(c) Finally, the Action Plan seeks to enhance the Financial Sector's Cyber Resilience through cyber threat workshops, and encouraging ESAs to develop cybersecurity supervisory practices and cyber resilience testing frameworks.

HONG KONG

Hong Kong's HK$50 Billion Investment in Innovation and Technology

On 28 February 2018, Financial Secretary for the Hong Kong Special Administrative Region, Mr. Paul Chan, unveiled Hong Kong's 2018 – 2019 budget. The budget includes a HK$50 billion investment in innovation and technology. The investment consists of the funding of the Hong Kong-Shenzhen Innovation and Technology Park; establishment of two research clusters on healthcare technologies and artificial intelligence and robotics technologies; further development of the Hong Kong Science Park to fund the construction of additional research-related infrastructure; additional funding for the Hong Kong Cyberport to boost support for start-ups and strengthen the Cyberport's incubation programme; and significant tax-reductions in domestic research and development expenditures.

INDIA

India Introduces New Regulations on Interconnection for Telecommunications

On 1 January 2018, the Telecom Regulatory Authority of India ("**TRAI**") introduced "The Telecommunication Interconnection Regulations" (the "**Regulations**"), which have subsequently come into force on 1 February 2018. Several telecommunication providers ("**TSPs**") provided representations to the TRAI to request that the legal and regulatory framework governing telecommunication interconnection be reviewed and updated. As such, TRAI prepared a pre-consultation paper and engaged in consultations with the TSPs to obtain their opinions on certain issues such as the situations where a TSP would be entitled to disconnect a point of interconnection. Based on this, TRAI formulated the Regulations which include, *inter alia*, provisions governing interconnection agreements entered into between the TSPs and interconnection charges.

UNITED KINGDOM

Proposed IoT Security Principles

On 7 March 2018, the Government released a policy paper titled "Secure by Design: Improving the cyber security of consumer Internet of Things Report" which contains a draft Code of Practice (the "**Code**") outlining proposed measures which manufacturers of Internet of Things ("**IoT**") should undertake to protect IoT devices from

cybersecurity risks. Some of the actions suggested by the draft Code include no default passwords; that companies should keep all IoT software updated; and that IoT device manufacturers should comply with applicable data protection regulations. The consultation on the draft Code will end on 25 April 2018.

Proposed Safety Standards for Smart Home Products

On 16 March 2018, the Government announced a consultation on a proposal on safety standards to be applied to smart home appliances. The proposal states various principles that manufacturers of connected appliances will need to consider, including but not limited to: interoperability (to ensure that all smart appliances may communicate with each other); data protection; grid-stability (to ensure that electricity usage is staggered to guard against any risk against the stability of the energy system); and cyber-security. The Government is intending for the standards to be aligned across both the EU and the USA, and stakeholders are invited to collaborate with the Government in the development of these standards. The consultation will be open until 8 June 2018.

UNITED STATES

CLOUD Act Becomes Law in the US

The Clarifying Lawful Overseas Use of Data Act ("**CLOUD Act**"), which has become law in the US, will provide the US government with greater access to the overseas data of Americans for the purposes of law enforcement. The CLOUD Act will allow any law enforcement official to be able to compel companies to release the required data, no matter where the data may be stored. The CLOUD Act also entitles the executive branch to enter into agreements with foreign countries which could permit each country to obtain personal data stored in the other countries, irrespective of the privacy laws of the other countries.

FBI Looks to Partner with the Private Sector in Managing Cybersecurity Risks

The Federal Bureau of Investigation ("**FBI**") Director, Christopher Wray has asked for greater collaboration between the FBI and the private sector in dealing with increasing cybersecurity risks. Speaking at a cybersecurity conference at Boston College in March 2018, the FBI Director requested that organizations inform the FBI upon discovering possible signs of cyberattacks. The FBI Director also mentioned that the FBI was trying to convey information relating to the *modus operandi* of cyber attackers and signs of cyberattacks to the private sector in a more effective manner. Crucially, the FBI Director highlighted that if companies were to disclose to the FBI that they were victims of a cyberattack, the FBI would do their best to assist these companies rather than passing on such information disclosed with other agencies that are investigating these companies on their regulatory compliance in protecting customer data.

CONCLUSION

We hope that this snap-shot of key TMT related issues occurring in the first quarter of 2018 has been useful. With the GDPR coming into force on 25 May 2018, the next quarter of 2018 will certainly bring about challenging (albeit exciting) times, in the ASEAN jurisdictions as well as in the rest of the world. And as always, do stay tuned for our next regional update as we bring to you the newest developments and updates on the TMT front.

For further enquires or discussion, please do not hesitate to contact our team below.

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) 28 3821 2382
F (84) 28 3520 8206

quang.chau@rajahtannlct.com

Vu Thi Que
Partner
Rajah & Tann LCT Lawyers

D (84) 28 3821 2382
F (84) 28 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

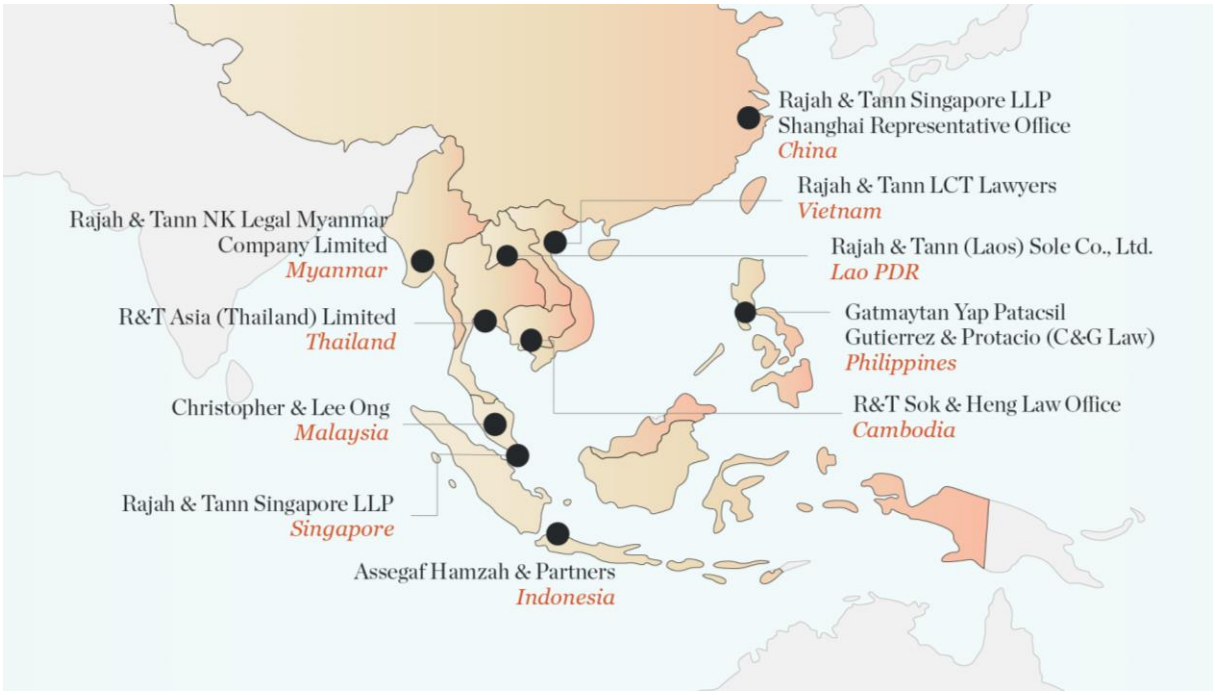
RAJAH & TANN LCT LAWYERS | *Vietnam*

Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382 / +84 8 3821 2673
F +84 28 3520 8206

Hanoi Office
T +84 24 3267 6127
F +84 24 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, the Philippines, Thailand and Vietnam. Our Asian network also includes regional desks focused on Japan and South Asia.