Technology, Media, And Telecommunications

Technology, Media and Telecommunications Regional Update

Introduction

As we approach the second-half of 2017, we are very excited to share with you the significant legal developments in the technology, media and telecommunications ("**TMT**") sector during the last quarter of 2016 and the first quarter 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.

ASEAN

SINGAPORE

Singapore launches Cybersecurity Strategy in October 2016

Singapore's Cybersecurity Strategy was introduced by Prime Minister Lee Hsien Loong on 10 October 2016 as he opened the Singapore International Cyber Week.

The Cybersecurity Strategy is intended to be a further step in securing Singapore's IT infrastructure and in bolstering trust in the same, and follows other recent cybersecurity related developments in Singapore, such as the establishment of the Cyber Security Agency of Singapore and the announcement that a new standalone cybersecurity legislation was in the process of being enacted.

The Cybersecurity Strategy sets out Singapore's vision, goals and priorities for cybersecurity, with a particular emphasis on protecting Singapore's "*critical information infrastructure*" and "*essential services*". To this end, the Singapore government has committed 8 percent of its ICT budget for cybersecurity.

In this regard, the Cybersecurity Strategy sets out four key pillars that form the basis of Singapore's strategy. These are:

(a) Strengthening the resilience of Singapore's "*critical information infrastructure*";
(b) Creating a safer cyberspace through a collaborative approach with businesses and the community, with a key focus on countering cyber threats, combating cybercrime and protecting personal data;
(c) Developing a vibrant cybersecurity ecosystem comprising of a skilled and equipped workforce, technologically-advanced companies and strong research collaborations; and

(d) Strengthening international partnerships to meet the evolving nature of cyber threats, which transcend jurisdictional borders.

Collaboration to Establish an Asia Pacific Regional Intelligence Centre

On 1 December 2016, the Monetary Authority of Singapore and the Financial Services Information Sharing and Analysis Center ("**FS-ISAC**") jointly announced a collaboration between them to set up an Asia-Pacific ("**APAC**") Regional Intelligence and Analysis Centre ("**the Centre**") to promote the exchange and analysis of cyber security information in the financial services sector within the APAC region. Against a backdrop of increasing cyber security threats around the world, the establishment of the Centre will help financial institutions located in APAC countries increase their resilience against such threats, by strengthening capabilities and providing support in terms of gathering, exchanging and analysing cyber intelligence within the region. To this end, local analysts employed at the Centre will identify, monitor and propose countermeasures against cyber security threats faced by member financial institutions. The Centre will be based in Singapore and was scheduled to commence operations within the first half of 2017 and we expect to further developments on the same shortly.

Spectrum for Fourth Mobile Operator Awarded

In mid-December 2016, the Info-Communications Media Development Authority ("**IMDA**") concluded the New Entrant Spectrum Auction and announced that TPG Telecom Pte Ltd ("**TPG**") had made the winning bid of S$105 million and would be provisionally allocated 60 MHz of spectrum to provide International Mobile Telecommunications ("**IMT**") and IMT-Advanced services (e.g. 4G services). This spectrum had been set aside for new entrant bidders (i.e., not an existing mobile network operator) in a bid to facilitate the entry of a new mobile network operator in Singapore. After the conclusion of the first stage of the General Spectrum Auction ("**GSA**") in early-April 2017, TPG was provisionally awarded 10 MHz of spectrum for the provision of high-speed mobile broadband services at a bid of S$23.8 million. Use of the spectrum to enhance networks could start as early as 1 July 2017. The next stage of the GSA will determine the specific spectrum bands to be allocated to the winning bidders.

Launch of 3D Printing Innovation Cluster

On 23 January 2017, Nanyang Technological University of Singapore ("**NTU**"), along with SPRING Singapore ("**SPRING**") and the Economic Development Board ("**EDB**"), officially launched the National Additive Manufacturing Innovation Cluster ("**NAMIC**") at NAMIC's inaugural Additive Manufacturing Summit. NAMIC was established as early as September 2015, way before its official launch, and is an innovation cluster which primarily focuses on 3D printing. NAMIC aims to reach out to companies interested in adopting 3D printing technology to help them overcome the high barriers of entry to 3D printing by providing them with funding and support and facilitating access to experts in the field as well as 3D printing facilities. NAMIC has since assisted nearly 400 companies in Singapore in their adoption of 3D printing technology for their businesses and aims to reach out to more than 1,000 companies over the next 4 years through various initiatives, such as workshops and industry events, to help them develop and innovate by using 3D printing technologies.

Deregistration of 2G-only Mobile Devices

With effect from 1 January 2017, the IMDA has de-registered 2G-only mobile devices for sale in Singapore. Equipment dealers may continue to sell 2G-only mobile devices for export purposes and/or overseas use only. This was in preparation for the 2G switch-off that took place in Singapore on 1 April 2017, whereby various mobile

operators in Singapore ceased the provision of 2G mobile services and shut down their 2G networks. The retirement of the legacy 2G networks will enable the scarce radio frequency spectrum to be reallocated for other purposes to meet consumers' demand for higher-speed mobile data and more advanced mobile services.

Helping SMEs Go Digital

At Budget 2017, the "SMEs Go Digital" programme was announced to help SMEs build stronger digital capabilities to seize growth opportunities in the digital economy. The building of strong digital capabilities was identified by the Committee on the Future Economy as one of the seven strategies to take Singapore forward. The "SMEs Go Digital" programme builds on the foundation of earlier programmes to incentivise SMEs to deploy technology-based solutions in their operations. Under the new programme, new digital capabilities such as cybersecurity, data protection, and data analytics will be included in addition to productivity tools such as digital ordering and payment, and fleet management. From 1 April 2017 onward, SMEs interested in participating in the programme can contact the IMDA or their nearest SME Centre for more information. In this regard, at the IMDA's inaugural "SMEs Go Digital" Industry Briefing held on 11 May 2017, it was announced that fifty digital solutions for SMEs have already been recognised in the "SMEs Go Digital" programme to increase SMEs' access to new technology.

Cybersecurity Breach in Ministry of Defence's System

In early February 2017, the Ministry of Defence ("**MINDEF**") detected a breach in its I-net system ("**I-net**"). Investigations revealed that basic personal data, comprising identification numbers, telephone numbers, and dates of birth of around 850 servicemen and employees were stolen as a result. MINDEF reported that no classified military information was stolen, as classified matters in the Ministry and the Singapore Armed Forces use a different computer system with more stringent security features and are not connected to the Internet. Upon detection, MINDEF disconnected the affected server from I-net and investigated all other computer systems within MINDEF/Singapore Armed Forces. MINDEF also informed the Cyber Security Agency and the Government Technology Agency of Singapore to investigate other Government systems.

McKinsey Sets Up Digital Capability Centre in Singapore

On 11 April 2017, McKinsey & Company ("**McKinsey**") opened a Digital Capability Centre ("**DCC**") in Singapore, located at the Clean Tech Park in the Jurong Innovation District. According to McKinsey, the DCC aims to help Southeast Asian companies tackle the challenges of, as well as capitalise on, emerging disruptive technologies (known collectively as "**Industry 4.0**"), which have the effect of enhancing data availability and connectivity, improving data analytics capabilities, facilitating human-machine interactions and creating new production methods such as 3D and 4D printing. The aforesaid objectives are achieved through the DCC by means of simulations of realistic production environments, digital showcases and hands-on capability building workshops. In line with Singapore's vision to become a regional hub for advance manufacturing, the DCC focuses on important industry sectors which include the discrete manufacturing, semiconductors, oil and gas, electric power, and mining sectors.

Cooperative Frameworks for Cross - Border Fintech Activities

The use of financial technology (known as "**Fintech**") has gained traction in Singapore since 2016, with the Singapore government pushing for the growth of Fintech by entering into partnerships with the governments of other countries. As of May 2017, the Monetary Authority of Singapore ("**MAS**") has entered into various cooperative agreements with the governments and other stakeholders of Abu Dhabi, Andhra Pradesh, France, Japan, South Korea, Switzerland and the United Kingdom. The cooperation frameworks established under these agreements will

support cross-border investments, expansion and collaboration between Fintech companies located in Singapore and the aforementioned countries, and allow financial regulators to cooperate and exchange regulatory views on the Fintech industry. With the Singapore government taking an active interest in the development of Fintech around the world, this is likely to be an industry with great potential and companies should watch the Fintech space so as to take full advantage of the commercial opportunities available.

Monetary Authority of Singapore Adopts Block Chain Technology

On 9 March 2017, MAS announced that it has successfully completed a proof-of-concept trial for the use of distributed ledger technology ("**DLT**"), which includes block chain technology, to facilitate domestic interbank payments. The project was undertaken by MAS in November 2016 in collaboration with R3, a DLT company, and various financial institutions. According to the MAS, the project has attained the goals of creating a digital representation of the Singapore dollar for interbank settlement, experimenting with the means by which banking systems may be linked to a DLT, and allowing interoperability between the MAS Electronic Payment System and DLT for automated collateral management. Through the project, MAS hopes to inspire industry players to make use of technologies like DLT to innovate and formulate new and improved solutions. MAS also plans to embark on further projects to enhance the efficiency of the fixed income securities trading and settlement cycle and formulate new methods for cross – border payments using digital currency.

PDPC Developing Certification Course for Data Protection Officers

On 13 March 2017, it was reported that the Personal Data Protection Commission (the "**PDPC**"), Singapore's regulatory authority responsible for the enforcement of the Personal Data Protection Act ("**PDPA**"), was developing a certification course for data protection officers, with a view of ensuring that data protection officers in Singapore are better equipped to take on their roles as the gatekeeper and primary steward of their organisation's personal data activities.

The designation of a person or persons to be responsible for an organisation's compliance with the PDPA (often referred to as the data protection officer(s)) is a requirement under the PDPA. However, to date, there has not been extensive guidance with regard to what qualifications are necessary for a data protection officer, or how data protection officers should be selected.

Hence, organisations generally tend to designate employees with existing roles as their data protection officers, as opposed to having a dedicated role for data protection officers. The certification course is also intended to promote the professional recognition of the role of data protection officer, and is consistent with the PDPC's intention for a greater professionalisation of the role of a data protection officer, as set out in the Cybersecurity Strategy released in October last year.

Further details are expected once the PDPC issues its official announcement in this regard.

Parliament passes Amendments to Computer Misuse and Cybersecurity Act

On 9 March 2017, the Computer Misuse and Cybersecurity (Amendment) Bill (the "**CMCA Bill**") was introduced in the Singapore Parliament. On 3 April 2017, the CMCA Bill was given its second reading in Parliament and passed.

The amendments are intended to ensure that the existing CMCA, which was last amended in 2013, remains relevant and capable of dealing and coping with the increasingly cross-border and global nature of cybercrimes (where the

perpetrators may not necessarily be, and are often not, located in Singapore) and the changing and evolving tactics of such cybercriminals.

To that end, key amendments introduced by the CMCA Bill are as follows:

(a) the creation of new criminal offences of dealing with personal data obtained illegally, or dealing with, obtaining and retaining items (such as computer programs) capable of being used, and intended for use, for the commission of computer misuse and cyber-related crimes under the CMCA;
(b) the granting of extraterritorial application of CMCA offences where it results in serious harm to Singapore (such as illness, injury or death of individuals in Singapore or disruptions to essential services in Singapore); and
(c) the allowing for multiple acts in which offences are committed to be combined into a single criminal charge (provided that the acts are all committed within a 12 month period). This is intended to allow the prosecution to view all the acts as a whole, rather than a series of acts and allow for any damage caused by the same to be calculated as a total and for the enhanced penalties to be imposed where the damage threshold is met.

Businesses and companies should now take note of these amendments, and take measures to ensure that these new offences are not unwittingly or inadvertently committed. Further developments in this area should also be monitored given that the new standalone cybersecurity legislation is intended to be introduced sometime this year as well.

MALAYSIA

Central Bank of Malaysia Expands Eligibility Criteria for the FinTech Regulatory Sandbox Framework

On 18 October 2016, following a one-month consultation on the proposed Financial Technology Regulatory Sandbox Framework (the "**Framework**") which was released on 29 July 2016, the Central Bank of Malaysia, i.e. Bank Negara Malaysia ("**BNM**"), issued details of the Framework which allows its participants regulatory flexibility to experiment with FinTech solutions in a “live” environment, subject to appropriate safeguards and regulatory requirements. During the course of the one-month consultation, BNM received over 60 comments and suggestions from various stakeholders including financial institutions, FinTech companies, associations and other corporate entities.

Following the comments and suggestions, BNM has introduced a new provision in relation to the eligibility criteria, thereby expanding the eligibility for applicants to participate in the sandbox. The new provision in question provides that where a FinTech company is considered to have the potential to contribute meaningfully to the creation of high value-added jobs in Malaysia, the company’s application to participate in the sandbox will be assessed more favourably by the BNM.

The Framework has since taken effect and is now open for application. BNM has stated that applicants should be able to demonstrate that a product, service or solution has been developed to a functional stage and is ready for testing. The applicants must also have a good understanding of the risks during testing, with adequate resources committed to effectively manage the risks. The finalisation of the Framework aims to provide an environment that is conducive for the deployment of FinTech to foster innovations in financial services that can contribute to the growth and development of Malaysia's financial sector.

Technology, Media, And Telecommunications

Relevant Authorities Urged to Review the Digital Signature Act 1997 and Electronic Commerce Act 2006

Deputy Communications and Multimedia Minister, Datuk Jailani Johari, has instructed the Malaysian Communications and Multimedia Commission ("**MCMC**") to review the Digital Signature Act 1997 (the "**Act**") which has not been amended since its coming into force in 1997. The Act is designed to make provisions for and to regulate the use of digital signatures. Under the Act, a digital signature is a legally binding signature with the effect that documents signed with a digital signature are as legally binding as a document signed with a handwritten signature, a thumbprint or any other mark.

According to the Minister, a study would need to be conducted by the Commission to determine the relevance and acceptability of the Act in view of the digital developments taking place in Malaysia. The Minister further added that when carrying out this study, the MCMC should seek involvement from the public, as well as all the stakeholders (including the three Licensed Certification Authorities appointed under the Act to carry out the prescribed services, i.e. to create digital identities and to issue digital certificates). The demand for digital certificates has seen a steady increase over the past few years, and is expected to continue to increase in 2017.

The Malaysian Ministry of Domestic Trade, Cooperatives and Consumerism is also proposing to review the Electronic Commerce Act with a view to protect consumers and traders who conduct businesses online, and to reduce fraudulent acts in online commercial transactions. The Electronic Commerce Act came into force on 19 October 2006 with the objective of enabling legal recognition of electronic messages in commercial transactions, the use of electronic messages to fulfil legal requirements and to enable and facilitate commercial transactions using electronic means.

Appointment of New Personal Data Protection Commissioner and Inclusion of New Classes of Data Users to be Registered under the Personal Data Protection Act 2010 ("PDPA")

The Minister of Communications and Multimedia has appointed Ms. Khalidah binti Mohd Darus as the new Personal Data Protection Commissioner with effect from 23 January 2017, pursuant to the powers granted under the PDPA.

In a related development, the Commissioner's office has also issued the Personal Data Protection (Class of Data Users) (Amendment) Order 2016 (the "**Amendment Order**"), which came into operation on 16 December 2016. The Amendment Order essentially adds to the list of entities that are required to register as data users under the PDPA, namely:

(a) in transportation sector, Malaysia Airlines Berhad;
(b) in utilities sector, Pengurusan Air Selangor Sendirian Berhad; and
(c) in other sectors, (i) Pawnbrokers (licensees under the Pawnbrokers Act 1972 (Act 81)); and (ii) Moneylenders (licensees under the Moneylenders Act 1951 (Act 400)).

In addition to the above, the personal data protection codes of practice for the utilities (electricity) sector, insurance/takaful sector, as well as the banking and financial sector, have recently been approved and registered by the Commissioner. The codes of practice set out the minimum standards of conduct in respect of personal data protection, drawn up respectively by the designated forums for the specific industries. Once registered, each code of practice will be binding upon all members of the relevant industries. A three-month grace period (from the date of approval and registration of the relevant code of practice) has been accorded to the respective members of the relevant industries in order to allow them to ensure that their internal processes are in line with the respective codes of practice. The enforcement phase is expected to commence from May 2017 onwards, and all data users are

expected to fully operationalise their data protection policies and procedures to be in line with the relevant codes of practice and/or the PDPA.

Government Efforts to Boost Malaysian Digital Economy

The Government of Malaysia has indicated its continued commitment to develop the digital economy through existing as well as new efforts which are to be implemented throughout 2017.

During the announcement for Malaysia's Annual Budget for Fiscal Year 2017, the Government has announced that RM 162 million (equivalent to USD 39 million) will be allocated for the development of a conducive "*e-commerce ecosystem*" in Malaysia. The Government has also announced plans to develop a Digital Free Zone ("**DFZ**") to provide for online and digital services to facilitate international e-commerce and internet-based innovations. The Government has also pledged to improve connectivity in Malaysia – fixed line broadband service providers will be expected to offer services at a higher speed for the same price, and Broadband speed is expected to increase up to 20 megabytes per second. To this end, MCMC will provide RM 1 billion (equivalent to USD 241 million) to improve the coverage and quality of broadband services throughout Malaysia.

In addition, the Malaysian cyber court was launched in September 2016 to regulate cyber activities, to facilitate the growth of the digital economy, and in particular, to address the increasing numbers of civil and criminal cyber offences. Datuk Seri Azalina Othman, a Minister in the Prime Minister's Department, has stated that judges and prosecution and defence counsels appearing in the cyber court must be "technologically-savvy", and proficient in cyber law and computer forensics. Although the cyber court is currently restricted to hearing only cases relating to cyber crimes, its jurisdiction is expected to be expanded to include hearing civil cases as well.

Proposed Regulations in Respect of Ride-Sharing and e-Hailing Services in Malaysia

It has been announced that the Parliament will be considering amendments to the Land Transport Act 2010 and Commercial Vehicles Licensing Board Act 1987 to regulate e-hailing services and the issuance of new taxi permits. One initiative proposed is the issuance of licences or new individual permits for existing taxi drivers to assist them in transferring from the taxi rental permit system. The terms and conditions under the existing taxi rental permit system will also be amended and upgraded to promote the welfare of taxi drivers. The new regulations will also include a blacklist of Uber or GrabCar drivers who break the law. Further, the Minister has urged taxi drivers to respond to consumers' increasing demand for e-hailing taxi services in ways other than viewing them as competition. Separately, the Deputy Transport Minister has criticised the growth of motorcycle e-hailing services, such as Dego Ride, as not only dangerous but also illegal as motorcycle taxis have not been licensed to provide such services.

Tabling of Amendments to the Communications and Multimedia Act 1998 in March 2017

The Malaysian Deputy Communications and Multimedia Minister, Datuk Jailani Johari, has announced the government's intention to table amendments to the Communications and Multimedia Act 1998 (the "**CMA**"). The Minister also stated that more than 300 stakeholders have been consulted during the review process thus far to assess the impact of the intended amendments. The MCMC is the primary agency responsible for the amendments, and has engaged the Attorney-General Chambers for their views on the amendments.

The review of the CMA is reportedly aimed at improving Malaysia's online environment, and in particular, online security. However, there are public concerns that the amendments to the CMA are intended to tighten the government's oversight of the online environment through creating additional offences and increasing existing

penalties, and may lead to the stifling of freedom of speech. In addressing these concerns and fears, Datuk Jailani has stated that the public should not be concerned as long as they use the internet properly and responsibly, and added that the review of the CMA does not only focus on the penalties provisions but also other areas "in line with the development of technology". This remains to be seen.

Malaysian Communications and Multimedia Commission Determination on the Mandatory Standard on Access ("Mandatory Standard")

The MCMC has published a revised Mandatory Standard on Access pursuant to its powers under the Communications and Multimedia Act 1998 ("**CMA**"). The Mandatory Standard came into force on 1 January 2017, setting out the general principles as well as mandatory regulated terms on key rights and obligations concerning inter-connection and access to network facilities or network services as listed under the CMA.

Under the Mandatory Standard, network facilities provider or network service provider licensed under the CMA ("**Access Providers**") are required to ensure that their terms and conditions of access are publicly available and in compliance with the Mandatory Standard. The terms and conditions must be capable of being signed as an access agreement or further negotiated by the Access Providers as well as Access Seekers (i.e. a person who makes a written request for access to the network facilities and/or services). The objective of the Mandatory Standard is to balance the need for expeditious and efficient access based on transparent terms, whilst providing flexibility to accommodate operator-specific matters and the interests of end users which may change over time.

As a consequence of the new Mandatory Standard, all Access Providers will be required to enter into Access Agreements based on the terms of the revised Mandatory Standards from July 2017 onwards, while all existing Access Agreements will need to be revised before the end of September 2017.

INDONESIA

Indonesia Implements Right to be Forgotten, Government to Stipulate Details

Towards the end of 2016, the Indonesian legislative parliament enacted Law No. 19 of 2016 ("**EIT Law Amendment**") on the Amendment to Law No. 11 of 2008 on Electronic Information and Transactions ("**EIT Law**"). The EIT Law Amendment addresses five main issues which includes, in particular, the right to be forgotten.

The right to be forgotten is a concept pioneered in Europe, which essentially refers to the right of an individual to request the removal of personal information from the Internet. Under the EIT Law Amendment, the right to be forgotten requires electronic system providers to erase electronic information or documents under its control which are no longer relevant, upon receiving a court order requested by the subject of the data in question. Electronic system providers must also establish an internal mechanism specifically on receiving, addressing, and processing a right to be forgotten request.

There are at least two main issues with the introduction of the right to be forgotten under the EIT Law Amendment. The first issue is in determining how 'relevancy' will be defined – will the Government provide guidelines or will it be left to the discretion of the court? The second issue is how the court order will be positioned – will it be compulsory for the right to be forgotten to be enforced? It is hoped that these issues will be addressed in the Government Regulation, which is the implementing regulation mandated to the EIT Law Amendment to further stipulate details in relation to the right to be forgotten.

For more information on the EIT Law Amendment, please refer to the publication from Assegaf Hamzah & Partners, "Electronic Information & Transactions Law Gets Makeover", at the following link: http://www.ahp.co.id/client-update-27-december-2016-2.

Personal Data Protection Rules Introduced, Albeit only for Electronic System Providers

MOCIT Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("**PDP Regulation**") was issued at the twilight of 2016. The PDP Regulation governs the protection of personal data but is restricted to those that are stored in electronic form and only applicable to electronic system providers. "Electronic system provider" is defined as "*any person, State authority, business entity or community that provides, manages, and/or operates an electronic system, whether independently or jointly, in the interest of the electronic system's users and/or the interests of other parties*". It should be noted that under this definition, electronic system providers include both private and public sectors (government authorities and state-owned enterprises) and has broad coverage, as it not only includes entities providing electronic systems but also entities managing electronic systems on behalf of a third party and entities operating an electronic system for their own internal purposes.

The PDP Regulation also elaborates on the definition of "personal data". "Personal data" is defined as "*certain data related to an individual, of which the (a) accuracy and (b) confidentiality is (i) kept, (ii) maintained and (iii) protected*". "*Certain data related to an individual*" is now further elaborated as "*all information that is correct and real, and personally identifiable, whether directly or indirectly, with an individual in accordance with the provisions of the laws and regulations in effect*". This means that any information that can be used to identify a specific person will be considered as personal data.

For more information, please refer to the publication from Assegaf Hamzah & Partners, "Personal Data Protection Regime Gets Boost with New Regulation", at the following link: http://www.ahp.co.id/client-update-29-december-2016.

Certification of Cellular Phones, Handheld Computers, and Tablets

Under Article 32 of Law No. 36 of 1999 on Telecommunication, every telecommunication device intended for use or sale in Indonesia must meet certain technical requirements provided by MOCIT. To meet such requirements, the devices manufacturer or its local importer is required to apply for device certification from MOCIT (**"Certification"**). The application for the Certification consists of two stages: the documentary check stage and the laboratory test stage. The time-consuming nature of the laboratory test stage had meant that the entry of telecommunication devices into Indonesia's market may be delayed.

To deal with this issue, MOCIT issued MOCIT Regulation No. 23 of 2016 on Certification of Cellular Phones, Handheld Computers, and Tablets ("**Devices Certification Regulation**"), which allows manufacturers and local importers to obtain the Certification without going through the laboratory test for cellular phones, handheld computers and tablet products ("**Devices**") which have been previously tested by the Cellular Telephone Industries Association ("**CTIA**"), Global Certification Forum ("**GCF**"), or other qualified local laboratories. Such certification process without the laboratory test stage is also known as the **Declaration of Conformity** procedure, and eligible applicants include the following:

(a) Trademark owners domiciled in Indonesia;
(b) Indonesia legal entities appointed by foreign trademark owners; and
(c) Indonesian legal entities that manufacture the Devices in Indonesia for a foreign trademark owner.

MOCIT Clarifies Liabilities of Platform Operators and E-Commerce Merchants

On 30 December 2016, MOCIT issued MOCIT Circular Letter No. 5 of 2016 on Limitations and Liabilities of Platform Operators and E-Commerce Merchants in the Form of User Generated Content ("**Platform Liabilities Circular**"), which specifically addressed the goods and/or services which may not be traded through user-generated-content platforms ("**UGC Platforms**"): (i) products containing negative content and (ii) illegal products. Examples of products containing negative content include pornography, gambling-related content, hatred-inciting content, and content that infringes the intellectual property rights of others, and examples of illegal products include, among others, weapons, explosives, prohibited drugs, protected animals, and hazardous chemicals.

The Platform Liabilities Circular also sets out the obligations and liabilities of UGC Platform operators, e-commerce merchants, and users. UGC Platform operators are subject to several obligations, among others, to set out clearly the terms and conditions which specify the types of content that can be uploaded by e-commerce merchants, and to actively evaluate and monitor the commercial activities carried out by their e-commerce merchants and users on their respective UGC Platform. E-commerce merchants, on the other hand, can be held liable for the content that they upload which violates the terms and conditions set out by the UGC Platform operator or under prevailing statutory laws and regulations. Where a UGC Platform operator is found to have failed to employ active monitoring measures and to act in a timely or effective manner in response to reports relating to listings of products containing negative content or illegal products, MOCIT may order internet service providers to temporarily or permanently block the UGC Platform in question.

App-Based Transportation Regulation Amendment in the Pipeline

In the world of app-based transportation where key players include Uber and Grab, the Indonesian government intends to issue a revision to the Minister of Transportation No. PM 32 of 2016 on Unscheduled Public Transportation Services ("**App-Based Transportation Regulation**") which was issued late last year following the mass demonstration by taxi drivers. The revision will address a number of matters in relation to app-based transportation, among which of particular scrutiny are in relation to taxation of app-based transportation and the provision of dashboard access to the Indonesian government.

It has been proposed that the App-Based Transportation Regulation be amended to mandate that app-based transportation service providers take the form of an Indonesian legal entity in Indonesia and to be subject to the following obligations:

(a) Directly enter into contracts, conduct sales or delivery of services, and invoicing in carrying out their business activities in Indonesia;
(b) Have an Indonesian bank account to be used to deposit proceeds from their business activities in Indonesia;
(c) Have or manage a server or data center domiciled in Indonesia;
(d) Carry out marketing and other promotional activities to support their business activities in Indonesia; and
(e) Provide a customer service center.

It has also been proposed that the Indonesian government be provided with dashboard access to achieve the ultimate objective of enabling government supervision, and the dashboard shall at least contain:

(a) The company profile of the app-based transportation service provider;

(b) Access to monitor the operational services of the app-based transportation service provider;
(c) Data of all public transportation companies with which the app-based transportation service provider has established operational cooperation;
(d) Data of all vehicles and drivers; and
(e) Customer service center details of the app-based transportation service provider.

THAILAND

Amendments to the Computer Crime Act 2007

The amendments to the Computer Crime Act took effect on 24 May 2017. Under the amendments, the powers of investigation and interrogation granted to the relevant officer have been extended to include powers of investigation into offences involving the use of computer systems, computer data, or computer data storage equipment under any laws (whereas previously the powers were limited to investigation into offences under the Computer Crime Act only). The officer would also be empowered to request the court to issue an order prohibiting the dissemination or removal of certain computer data from computer systems (for example, computer data that infringes on the intellectual property rights of others or that is contrary to public policy).

The amendments introduced a new offence for sending disturbing computer data or electronic mail to another person without providing the recipient with an option to unsubscribe. There are also new provisions requiring a service provider to retain computer traffic data for up to 2 years from the date that such data enters into the computer system.

Draft Cybersecurity Bill

Several years ago, the government introduced a draft Cybersecurity Bill ("**Bill**") to promote the digital economy in Thailand. The Bill was approved by the National Reform Steering Assembly on 28 November 2016, and will be submitted for the consideration of the Cabinet, the Council of State, and the National Legislative Assembly before enactment. The main objective of the Bill is to establish the National Cybersecurity Committee ("**NCSC**"), which will be responsible for setting cybersecurity measures to prevent and manage cyber risks that may affect the provision and implementation of computer systems, internet, telecommunication platforms, or satellites.

The existing draft Bill has been the subject of some concern, in particular, regarding the broad powers granted to the relevant officer to gain access to information sent through the post, telephones, computers, and other devices without the need to obtain a court order to do so. This issue is likely to be the subject of further debate by the legislators in the near future.

NCPO's Initiative to Grant More Patents

On 28 February 2017, the National Council for Peace and Order ("**NCPO**") conferred on an issue regarding the delays in the patent prosecution process, which has resulted in a backlog of over 12,000 pending applications in the past 10-20 years. In order to increase investor confidence, the NCPO decided to exercise its constitutional power to grant a patent for an application which has been pending for 5 years or more, provided that the product which is the subject of the pending patent application (i) has actually been produced in accordance with the specification in the application, and (ii) a patent has been granted in another country for a corresponding application.

The date for implementing this measure has not yet been set, but is likely to result in up to 10,000 patents being granted within 3 months after implementation.

VIETNAM

Key Information Technology Products

On 16 February 2017, the Ministry of Information and Communications ("**MIC**") issued Circular No. 01/2017/TT-BTTTT ("**Circular 01**") which took effect on 2 April 2017. Circular 01 sets out a list of key information technology products for the purposes of constituting key information technology products systems, assisting in investment activities application of tax and incentive policies, import and export management, quality management and other activities relating to other activities related to those key information products.

'Key information products' are defined as products satisfying one of the following requirements: (i) having a great demand in the domestic market or creating a high added value; (ii) having export potential; (iii) having positive impacts on technological renewal and having economic efficiency for other economic sectors; or (iv) meeting defense and security requirements. Pursuant to Circular 01, the list of key information technology products includes the following products:

(a) Receiver/transmitter/signal converter equipment to be used in 2nd generation digital video broadcasting and the next generation;
(b) Ipv6 equipment;
(c) RFID tag and RFID reader equipment;
(d) Open IoT platform software;
(e) Open big data analysis platforms software;
(f) Open e-Government platforms software; and
(g) Information safety product.

The list will be updated and supplemented by the practical requirements and announced in the Portal of the MIC from time to time.

New Regulations on Electronic Games for Foreigners

On 30 December 2016, the Government issued Decree No. 175/2016/ND-CP to amend and supplement some articles of Decree No. 86/2013/ND-CP dated 29 July 2013 on business in prize-winning electronic games for foreigners ("**Decree 175**"). The Decree 175 took effect on 15 February 2017.

According to the Decree 175, electronic game machines must be 100% new with technical specifications announced by manufacturers and verified by G7-based independent certification organisations. In addition, payout rates of slot machines installed in gaming facilities must be at least 90%. In relation to the conditions for the Business Eligibility Certificate, Decree 175 states that equity capital of entities licensed to offer their electronic game machines to customers to play shall be no less than VND 200 billion (approx. USD 8,770,000).

New Circular Stipulating the List of Digital Information Content Products

On 26 December 2016, MIC issued Circular No. 43/2016/TT-BTTTT sets out the list of digital information content products ("**Circular 43**"). Circular 43 took effect on 10 February 2017.

The list of digital information content products systematises the specialised industry products with digital content to serve as grounds for investment activities, application of tax and incentive policies, import and export management, quality management and other activities relating to digital information content products. Digital information content products include:

(a) Digital products for education;
(b) Digital books and documents;
(c) Entertainment and education products on mobile and landline telecommunication networks;
(d) Electronic games;
(e) Digital library and digital data storage;
(f) Digital film, picture, music and advertising; and
(g) Other digital information content products.

The list of digital information content products will be updated and supplemented subject to the market developments, telecommunication development policy and management requirements from time to time.

New Regulations on Standard Form Contracts in the Telecommunications Sector

On 26 December 2016, MIC issued Circular No. 39/2016/TT-BTTTT regulating the provision of standard form contracts in the telecommunications sector, which took effect on 15 February 2017 ("**Circular 39**"). Under Circular 39, telecommunication services fall into: (i) telecommunication services for which applicable standard form contracts must registered; or (ii) telecommunication services for which applicable standard form contracts must be notified to the authorities.

Standard form contracts for: (i) landline telephone services; (ii) land mobile information services; and (iii) internet access service on landline telecommunication network must be registered with the Ministry of Industry and Trade or the relevant Department of Industry and Trade.

Standard form contracts for: (i) fixed telecommunications services such as private leasing channel services, data transmission services, video conferencing services, virtual private network services and (ii) other telecommunications services must be notified to the MIC.

In addition, standard form contracts for telecommunication services must be made in writing in Vietnamese and have minimum contents as stipulated by the Circular 39.

New Circular on the Cross-Border Provision of Public Information

On 26 December 2016, the MIC issued Circular No. 38/2016/TT-BTTTT providing detailed regulations on the cross-border provision of public information, which took effect on 15 February 2017 ("**Circular 38**"). Under Circular 38, an offshore entity that provides cross-border public information into Vietnam and: (i) has more than 1 million views from Vietnam per month; or (ii) leases a data centre to store digital information in Vietnam in order to provide its services, must provide certain contact information (which includes but is not limited to its registered name and country, the address of its head office, nationality and contact point of the offshore service provider) to the MIC.

Circular 38 also specifically implements the content restrictions provided for under Article 5 of Decree No. 72, in which the use and provision of the internet should not, inter alia, oppose the Socialist Republic of Vietnam, threaten

national security, incite violence, arouse racial and religious animosity, propagate pornography or contradict national traditions ("**infringing content**"). If the MIC identifies infringing content on a forum provided by an offshore service provider, the MIC will apply the necessary preventative measures.

Telecommunication enterprises and onshore data centre service providers are required to report infringing content by direct submission, post or email to the MIC within 3 hours of discovery. In addition, onshore data centre service providers must either periodically or upon the MIC's request notify the MIC of the services that they supply to offshore service providers.

CAMBODIA

Draft Prakas on Telecommunications Licensing Regime and Draft Prakas on Telecommunications Licensing Fees

As part of implementing the Law on Telecoms, the Telecommunication Regulator of Cambodia organised a public consultation on 20 February 2017 on two draft Prakas: (i) Conditions and Legal Procedures of Granting, Modification, Suspension, Transfer and Withdrawal of Permit, Certificate and License of Telecommunications Operations ("**Draft Prakas on Telecoms Licensing Regime**"); and (ii) Determination of Fees of Permit, Certificate, License and Relevant Fees in Cambodia ("**Draft Prakas on Telecoms Licensing Fee**").

Under the Law on Telecoms, telecommunications operations are subject to the permit, certificate and license requirements pursuant to the Article 15, Article 16 and Article 17 respectively. The Draft Prakas on Telecoms Licensing Regime suggests a new and simpler telecommunications licensing regime by consolidating all telecommunications licenses into three main categories as follows: (i) licence on infrastructures and services; (ii) licence on limited infrastructures and services and (iii) licence on services. Further, the Draft Prakas on Telecoms Licensing Fee prescribes (i) the administrative fee for application study for permit, certificate or license; (ii) the annual fee of permit, certificate or license; and (iii) security deposit for execution in case of application for license.

Telecommunications operators were invited to provide comments on the draft Prakas by 24 February 2017.

Draft Regulations in the Sector of Information, Communication Technologies

In response to the developing business operations in the sector of Information, Communication Technologies ("**ICT**"), Ministry of Posts and Telecommunications of Cambodia ("**MPTC**") has initiated (i) the Draft Prakas on Authorization for Business Conduct in the Sector of ICT ("**Draft Prakas on ICT Authorization**") and (ii) the Draft Sub-Decree on digital signature ("**Draft Sub-Decree on Digital Signature**"). The Draft Prakas on ICT Authorization confers the General Department of ICT ("**GDICT**") and the MPTC with certain powers, including the power to issue permits, certificates and licences. The Draft Sub-Decree on Digital Signature is currently being drafted to promote and strengthen the efficiency and security of digital signature usage in Cambodia.

Universal Service Obligation ("USO") and Capacity Building Research and Development ("CBRD") Funds

Following the last workshop on USO and CBRD Funds arranged by MPTC on 6 October 2016 with all key stakeholders, MPTC has prepared two drafts Sub-decrees for both USO and CBRD respectively and arranged two rounds of pubic consultations with all key stakeholders, including private sectors, to collect their inputs and comments on the legal instruments. The last consultation workshop took place on 19 December 2016 and the drafts are currently being reviewed and revised by MPTC.

It should be noted that the draft Sub-decrees are also part of the implementation of the Law on Telecoms under which all telecommunications operators are required to contribute in the amount equivalent to 2% and 1% of their gross revenue into the USO Fund and CBRD Fund respectively.

THE PHILIPPINES

Newly Established Philippine Department of Information and Communications Technology ("DICT") Issues its Implementing Rules and Regulations ("IRR") and Drafts the National Cybersecurity Framework

On 17 October 2016, the DICT issued the IRR of Republic Act No. 10844 which transfers to the DICT government agencies, units, and offices with functions and responsibilities dealing with communications. In this regard, the IRR expressly provides that, for purposes of policy and program coordination, the National Telecommunications Commission, National Privacy Commission, and Cybercrime Investigation and Coordination Center ("**CICC**") shall be attached to the DICT.

In addition, the DICT, through the CICC, released a draft National Cybersecurity Framework intended to provide a coherent set of implementation plans, programs and activities to be shared with the public and private sectors, the civil society, and the academe including private individuals, to secure Philippine cyberspace against various threats, including cyber criminals, terrorists, and hacktivists. The DICT called on stakeholders to provide input and feedback on the Framework.

The Philippine Commission on Elections ("COMELEC") Confirms Theft of Computer Containing Millions of Voter Records

The COMELEC has confirmed that a computer containing the National List of Registered Voters ("**NLRV**") and certain biometric records was stolen in Lanao del Sur, a province in Southern Philippines. Pending investigation, the National Privacy Commission ("**NPC**") ordered COMELEC to destroy copies of the NLRV in its computers if it cannot secure the same and to inform all data subjects affected by the potential data breach. NPC also ordered COMELEC to submit its proposed revisions to the Philippine voter registration process to be in line and compliant with the provisions of the Data Privacy Act of 2012, its implementing rules and regulations, and other related NPC circulars.

This is another major setback for the agency. The NPC had previously recommended the prosecution of COMELEC Chairman Andres Bautista for violating the provisions of the Philippine Data Privacy Act in connection with the massive data breach that occurred between 20 and 27 March 2016. The COMELEC has filed a Motion for Reconsideration, which is still pending before the NPC.

Credit Card Industry Regulation Law Passed; Implementing Rules and Regulations to Follow

The Philippines passed Republic Act No. 10870 or the Philippine Credit Card Industry Regulation Law governing all credit card issuers, acquirers and credit card transactions in the country. It seeks to protect credit card holders against credit card fraud and unfair practices of credit card issuers and acquirers. In this regard, credit card issuers are now required to, among other requirements, notify cardholders of important information on the credit card including those related to finance charges, interest rates, and penalties. Issuers are likewise required to undertake due diligence measures to ascertain the identity of cardholders and to secure the proper collection, use, and

disclosure of cardholder data. The new law also expressly provides that all credit card issuers and acquirers shall be under the supervision of the Philippine Central Bank.

Philippine President Rodrigo Duterte Approves National Broadband Plan

Philippine President Rodrigo Duterte has approved the national broadband plan proposed by the Department of Information and Communications Technology, emphasising the need for faster communications in the country. The plan was passed with a view to accelerate the deployment of fiber optic cables and wireless technologies in the country to improve internet speed. The project is expected to cost as much as two hundred billion pesos (PhP200,000,000,000.00) and will take approximately three (3) years to complete.

Philippine Telecoms Companies Ink Deal to Lower Interconnection Rates

The National Telecommunication Commission of the Philippines issued Memorandum Circular No. 09-11-2016, which directed that interconnection rates among telecommunication companies' voice services should not be higher than two pesos and fifty centavos (PhP 2.50) per minute from the previous four pesos (PhP 4.00) per minute. In this regard, the Department of Information and Communications Technology, PLDT Inc. and Globe Telecom signed a memorandum of agreement ("**MOA**") to lower interconnection charges in a bid to reduce the rates of mobile and fixed line calls in the country. The MOA took effect on 1 January 2017.

REST OF ASIA-PACIFIC

AUSTRALIA

Use of Blockchain Technology to Combat Food Fraud

On 24 March 2017, Alibaba Australia announced that it has entered into a memorandum of understanding with Australia Post, PricewaterhouseCoopers and Blackmores for a pilot project to create a new tracking system for food deliveries across the supply chain through the use of blockchain technology (amongst other technologies).

The aim of the pilot project is to combat fraud and counterfeit food products, strengthen the ability to trace food deliveries, safeguard Australia's reputation as a trusted exporter of food, and facilitate the safe delivery of Australian food products to Chinese consumers. Blockchain technology will play a significant role in this pilot project, as it acts as a database containing information on where and how food was grown and facilitates the tracking of food movements across the supply chain. It is hoped that this pilot project will result in a global supply chain model which can be applied to all of the Alibaba Group's e-commerce markets and ultimately build public confidence in the purchase of food online.

Australian Government Looking to Spend AU$900 million on Australian Tech Start-Ups

On 20 March 2016, the Assistant Minister for Digital Transformation, Angus Taylor, announced his plan to allocate 10% of the annual budget for technology spending for the public sector, amounting to AU$ 900 million (approximately S$ 954 million), on small local tech companies, as opposed to dominant players such as the likes of IBM, SAP, and Hewlett-Packard. While no detailed timeline has been proposed, Taylor said that he wished to implement this plan as soon as reasonably practicable, referring to the government's efforts as "probably the biggest investment in innovation in this country's history". The plan will involve a fundamental change in the way the public

sector awards contracts to tech companies – by selecting tech providers from a new government digital marketplace as opposed to choosing within a group of pre-selected providers. This is a laudable move by the government, which no doubt opens up a wealth of opportunities for smaller tech companies and start-ups in Australia to grow and expand.

Launch of Australian Landing Pad in Singapore

On 13 March 2017, the Australian government launched the Australian Landing Pad ("**ALP**") at One-North in Singapore. The ALP is the most recent initiative under a strategic partnership entered into between Australia and Singapore in 2015. It allows Australian start-ups to gain access to collaborative workspaces for a maximum of 90 days by providing support through education, mentorship and financing. Candidates will be selected by the Australian Trade Commission after evaluating their track record and their capabilities in terms of expanding and differentiating themselves in the market. Not only will Australian start-ups stand to gain from this initiative, aspiring entrepreneurs in Singapore can also take advantage of this opportunity to work with their Australian counterparts to build start-ups in Singapore. Singapore is one of the five global innovation hubs identified by the Australian government for the project, the others being San Francisco, Tel Aviv, Shanghai and Berlin.

PEOPLE'S REPUBLIC OF CHINA

Google Reportedly Looking to Return to PRC

Google's on-again, off-again dalliance with returning to the People's Republic of China ("**PRC**") following their exit over censorship issues 7 years ago may be a step closer to reaching fruition, as a senior PRC official issued a press statement on 12 March 2017 indicating that various elements of the PRC government have been in touch with Google over the past year. Liu Binjie, a standing committee member of the PRC National People's Congress and former head of the General Administration of Press and Publication, informed press representatives that a staggered approach is being considered, with the parts of Google's business that pose a lower socio-political risk in the eyes of the PRC regime, such as Google Scholar, for example, being earmarked to re-enter the PRC domain first. No clear timetable has been set for Google's return as yet, but it will be interesting to observe the extent to which Google will be willing to compromise on its vaunted corporate values in order to gain access to the highly lucrative PRC market.

Fintech Continues to Be a Key Driver of PRC Consumer Economy

Fintech continued to be a key economic driver in the PRC in 2016, with technological innovations and an increased level of mobile penetration fueling strong growth in consumer spending. The PRC has long been viewed as the undisputed world leader in fintech, accounting for nearly half the global total of digital payment transactions and approximately three-quarters of the global market for online lending, and early analyses indicate that 2016 would be no exception to this assessment. This was evinced by the value of mobile payment transactions in the PRC in the first three quarters of 2016 more than doubling to 22.5 trillion yuan compared to the same period of 2015, and also by the value of online retail sales increasing by 26.2% to 5.16 trillion yuan in 2016 (compared to only a 10.4% growth in total retail sales). Experts observe that this growth in consumer spending is attributable to the ease and convenience with which online and mobile purchases may be made, with the easy availability of interest-free loans proving to be a strong incentive to making expensive purchases. The advent of fintech has also coincided with a shift in generational mindsets in the PRC, with the increasingly affluent younger middle-class abandoning the frugal attitudes of their elders in favour of a more generous consumer mindset.

Technology, Media, And Telecommunications

HONG KONG

Hong Kong Court Issues Landmark Ruling against Uber Drivers

Another salvo in the ongoing battle between Hong Kong state authorities and Uber was fired on 10 March 2017, as five Uber drivers were each convicted by the West Kowloon Court of one count of driving a vehicle for hire without a permit and one count of using a vehicle without third-party insurance. In the highly anticipated verdict, each driver was fined HK$10,000, banned from driving for one year, and had the smartphones and/or tablets they used to commit the offences confiscated. All five of the drivers have since indicated that they intend to appeal their convictions and sentences.

The thorny issue of how and to what extent Uber and other disruptive ride-sharing businesses should be regulated is one that is being faced by government authorities across the world. Hong Kong has not introduced any specific legislation or regulation targeting this issue, choosing instead to rely on existing regulations relating to safety and permits. It is notable that the five Uber drivers were convicted under a provision in the Road Traffic Ordinance that was introduced in 1977 in order to combat the spate of illegal taxi drivers prevalent at that time, as it raises the pertinent question of whether such an old and outmoded law can be relevant or applicable in relation to modern ride-sharing apps and businesses. Observers have also noted that the relevant permit requirements are completely out of sync with Uber's app-based business model, meaning that Uber drivers cannot possibly obtain a permit even if they applied.

Even as commentators note that this court judgment is likely to signal a further crackdown on Uber's business in the coming months, Uber remains defiant in the face of this setback, with its Hong Kong general manager issuing a strong statement outside the courts that Uber will continue to fight for its ride-sharing business to be legalized in Hong Kong.

INDIA

TRAI Issues Consultation Paper on Net Neutrality

In our previous update, we highlighted that the Telecom Regulatory Authority of India ("**TRAI**") had issued a pre-consultation paper on net neutrality. TRAI has since followed this up by issuing a full consultation paper on 4 January 2017, to assist it in deciding on the extent of regulatory intervention required to ensure the protection of net neutrality in India and minimise discriminatory treatment in the provision of access to the Internet.

TRAI has considered the following issues in the consultation paper:

(a) How to ensure that traffic management practices implemented by ISPs are reasonable and non-discriminatory in nature;
(b) Identification of the core principles of net neutrality;
(c) Whether transparency-related obligations should be imposed on ISPs;
(d) Whether a monitoring framework should be established and to what extent; and
(e) Which regulatory instruments should be used to implement the net neutrality framework in India.

The closing date for the consultation paper has been extended twice, and stakeholders were given until 12 April 2017 to provide their comments and input.

Safe Harbour for Online Intermediaries Recognised by Delhi High Court

On 23 December 2016, the Division Bench of the Delhi High Court issued its decision in the case of *Myspace Inc v Super Cassettes Industries Ltd*. In that case, Super Cassettes brought an action against Myspace for copyright infringement, on the basis that the songs and media content which Myspace's users uploaded on its website violated Super Cassettes' copyright.

At the first instance, the High Court held that Myspace was indeed liable for copyright infringement. However, on appeal, the Division Bench reversed the lower court's decision, and held that Myspace would not be guilty of copyright infringement, as:

(a) Myspace did not have actual knowledge that the uploaded content infringed Super Cassette's copyright; and
(b) Myspace could avail itself of the safe harbour provisions in the Information Technology Act, in light of its existing systems to protect copyright (including a notice-and-takedown system, and a rights management tool).

Nevertheless, Super Cassettes could still protect its content by providing Myspace with a notice containing specific details and the location of the content in question, which Myspace would then have to remove within 36 hours. This case is important as it establishes an appropriate balance between the protection of online intermediaries and the need for copyright owners to protect their content.

REST OF THE WORLD

EUROPEAN UNION

European Parliament Passes Resolution Calling for Legislative Proposals to Regulate Robotics and Artificial Intelligence

The development and increased usage of robotics and artificial intelligence ("**AI**") raises various legal, social and ethical concerns and challenges that prompt the need for a legal framework that is appropriate and adequate to safeguard and protect human well-being and human rights while not hindering innovation.

On 16 February 2017, the European Parliament passed a resolution requesting the European Commission ("**EC**") to propose civil law rules on robotics to address issues such as intellectual property rights, data ownership, employment and liability, and to adopt detailed recommendations in the Report with Recommendations to the Commission on Civil Law Rules on Robotics. Some of the detailed recommendations include but are not limited to:

(a) Establishing the definition of 'smart autonomous robots' to be applied EU-wide;
(b) Introducing a registration system for advanced robots;
(c) Clarifying civil liability rules for robots causing damage, which should not restrict the type or extent of damages that may be recovered or the forms of compensation that may be sought (other than for damage to property); and
(d) A proposed Code of Ethical Conduct for Robotics Engineers covering research and development activities in the robotics field.

It should be noted that while the resolution passed by the European Parliament is non-binding in nature, the EC will have to justify any decision not to proceed with the draft legislation.

EU Ambassadors Confirm Provisional Agreement on Regulation Regarding Cross-Border Portability of Digital Content Services

In this digital age, the unhampered access to and use of online services and content regardless of location is highly coveted by consumers. On 15 February 2017, the Presidency of the Council of the European Union ("**EU**") reached a provisional agreement with the European Parliament to remove barriers to cross-border portability of online content services within the EU market. Under the proposed Regulation on Cross-Border Portability of Online Content Services in the Internal Market ("**Regulation**"), consumers who have subscribed to or paid for online content services in their home country will be allowed to access such services when temporarily staying in another country within the EU. The Regulation, if formally approved by the Council of the EU and the European Parliament, will become applicable nine months following its publication in the EU's Official Journal.

UNITED KINGDOM

UK Publishes Digital Strategy

On 1 March 2017, the government of the United Kingdom ("**UK**") published its Digital Strategy which aims to make UK's digital economy stronger and fairer as the UK prepares to leave the European Union.

The Digital Strategy contains 7 main components:

(a) Building world-class digital infrastructure for the UK;
(b) Giving everyone access to the digital skills they need;
(c) Making the UK the best place to start and grow a digital business;
(d) Helping every British business become a digital business;
(e) Making the UK the safest place in the world to live and work online;
(f) Maintaining the UK government as a world leader in serving its citizens online; and
(g) Unlocking the power of data in the UK economy and improving public confidence in its use.

The Digital Economy will act as an impetus for continued close cooperation and engagement between the UK government and the technology industry and sectors to support the growth of the UK digital economy. As the UK government will be looking to create a strong data infrastructure and ensuring a high level of regulatory compliance, companies should ensure that their operational and internal policies are adequate to prepare them for the developments ahead.

New Code of Practice to Tackle Online Piracy

On 20 February 2017, the UK Intellectual Property Office ("**IPO**") assisted with brokering a deal in which search engines such as Google and Bing and the creative industries agree to co-operate to tackle online piracy under a voluntary Code of Practice which came into immediate effect. As search engines are a key avenue in which consumers access and uncover online content, the Code of Practice seeks to prevent consumers from being led to copyright infringing sites through search results by removing links to such sites from the first page of search results.

UNITED STATES

Facial Recognition Technology Used by FBI Called into Question

On 22 March 2017, the Full House Committee on Oversight and Government Reform ("**Committee**") presented findings from its review on the use of facial recognition technology ("**FRT**") for law enforcement. The Committee found that nearly half of the photographs of Americans are stored in an FRT database which can be accessed by the Federal Bureau of Investigation ("**FBI**") without their consent or knowledge, and 18 US states have entered into memorandums of understanding with the FBI to share photos with the government. Some issues arising from the use of FRT include the possibility of misidentification and racial bias. Further, the Committee found that in using FRT, the FBI has tried to exempt itself from various provisions of the US Privacy Act, including the legal requirement to publish a privacy impact assessment. The problems associated the use of FRT, coupled with a lack of legal controls, raises serious concerns in relation to the accountability over the use of FRT for law enforcement. Therefore, the Committee and other commentators have identified the need for regulation and protection of privacy.

Federal Communications Commission ("FCC") Pauses Implementation of a Broadband Privacy Rule

On 1 March 2017, FCC Chairman Ajit Pai and Acting Federal Trade Commission ("**FTC**") Chairman Maureen K. Ohlhausen issued a joint statement regarding the FCC's issuance of a temporary stay of a data security regulation, before it could take effect on 2 March 2017. According to the joint statement, both Chairmen expressed the intention for jurisdiction over broadband providers' privacy and data security practices to be returned to the FTC. Until that happens, the FCC and FTC will work together on harmonising the FCC's privacy rules for broadband providers with the FTC's standards for other companies in the digital economy. As such, the FCC paused the implementation of the privacy rule that is inconsistent with the FTC's privacy framework. The stay will remain in effect until the FCC is able to rule on a petition for the reconsideration of its privacy rules.

U.S. Department of Commerce Releases Green Paper Proposing Approach for Advancing Growth of Internet of Things

The U.S. Department of Commerce released a report on 12 January 2017 proposing actions that the Department can take to realise the full potential of the Internet of Things ("**IoT**"). The green paper examines the benefits and challenges of the evolving IoT landscape and identifies four broad areas of engagement related to IoT: (i) enabling infrastructure availability and access; (ii) crafting balanced policy and building coalitions; (iii) promoting standards and technology advancement; and (iv) encouraging markets (such as through public-private partnerships). The U.S. government will continue engaging with stakeholders so as to craft policy that will help to foster an innovative IoT environment that protects individuals.

Conclusion

This wraps up our summaries of the various interesting and exciting TMT issues that have arisen at the end of 2016 and early 2017. We are happy to have been able to provide this summary for you, and we hope that you have found this overview useful. 2017 promises to be an exciting year, particularly with the initiatives introduced by the Singapore government during the Budget 2017 speech as well as with the various jurisdictions in the ASEAN region having so many developments in this area, so do stay tuned to our next update on the important developments in the TMT sphere.

Contacts

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

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

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

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

Lionel Tan
Partner, Technology, Media & Telecommunications
Rajah & Tann LLP Singapore

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

Benjamin Cheong
Partner, Technology, Media & Telecommunications
Rajah & Tann LLP Singapore

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

Tanya Tang
Partner (Chief Economic and Policy Advisor), Competition & Antitrust and Trade
Rajah & Tann LLP Singapore

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

Mary Thel T. Mundin
Partner
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

Mohd Zulkifli Intan Haryati
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

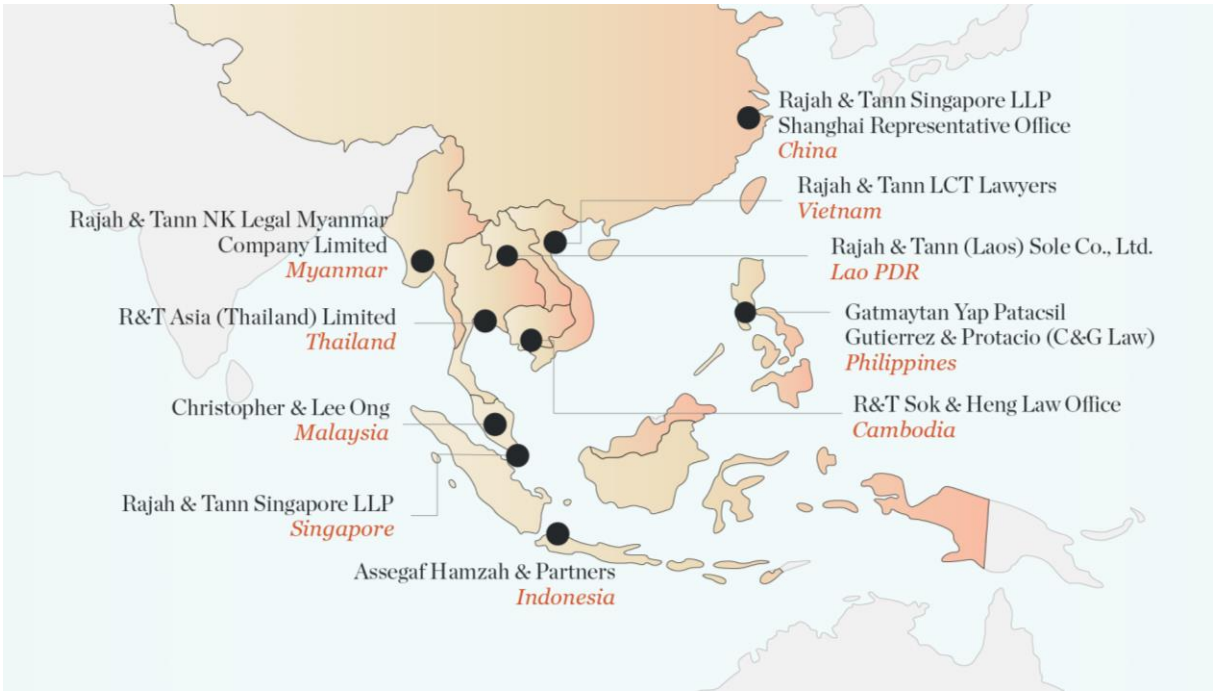
RAJAH & TANN LCT LAWYERS | *Vietnam*

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.