Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Asia Pacific

Gabriela Kennedy

Partner, Mayer Brown, Hong Kong

CLSR Vol. 37.1

1. China

1.1. *Third Times a Charm – Further Draft Amendments Issued for the PRC Personal Information Security Specification*

On 24 October 2019, a third round of draft amendments ("**Third Draft** ") to the "Information Technology – Personal Information Security Specification" (National Standard GB/T 35273-2017) (GB/T 35273-2017 信息安全技术 个人信息安全规范) ("**Specification**") were issued. This Third Draft follows two earlier versions that had been released for public consultation on 1 February 2019 and 25 June 2019.

The original Specification came into effect on 1 May 2018, and sets out recommended best practices for the protection of personal information. Even though the Specification does not have the force of law, the PRC authorities take into account any non-compliance when carrying out investigations or enforcement actions (e.g. in relation to the PRC Cybersecurity Law).

The Third Draft provides further clarification and some additional restrictions not seen in the earlier versions of the draft amendments. The following are some of the latest key changes introduced by the Third Draft that do not appear in the previous versions.

1.1.1. *No forced consent due to improvements*

Individuals cannot be obligated to provide their consent to the collection of their personal information on the basis of receiving an improved quality of service or security, enhanced user experience or for the development of any new products;

1.1.2. *Users' termination of online services*

Data controllers must comply with the following requirements regarding their users' ability to terminate their subscription for online services:

(a) provide an interface that enables the user to easily unsubscribe from further receipt of the services;
(b) comply with any termination request within 15 days;
(c) for the purposes of verifying the identity of the user, not collect any additional personal information above what has already been collected by the data controller during the registration process and provision of the services;
(d) specify how sensitive personal information, which was collected for the purpose of identity verification in relation to the cancellation of the services, shall be dealt with; and
(e) not impose any unreasonable conditions or additional requirements on users in relation to termination of the services.

1.1.3. *Remedial steps to be taken in the event of a data processor's breach*

A data controller must take appropriate remedial steps (including, where necessary, terminating its agreement with the data processor and requiring it to delete all personal information provided), if its data processor fails to process the personal information pursuant to the relevant agreement with the data controller, or fails to implement adequate measures to protect the personal information.

1.1.4. *Joint data controllers*

If personal information is under the joint control of 2 data controllers, then the data controllers must execute an agreements setting out their respective obligations, including in relation to security and data breach notifications. A data controller shall remain liable and responsible for the actions of its joint data controller, if it fails to notify the data subjects of the identity of the joint data controller and their relevant obligations regarding the personal information collected.

Takeaway

The PRC authorities are continuing to take a proactive role in enforcing any data breaches involving personal information under various laws, including the PRC Cybersecurity Law. While the Specification does not have the force of law, once finalised and issued, the amendments introduced by the Third Draft will provide a clear indication of what the PRC authori-

E-mail address: gabriela.kennedy@mayerbrown.com

https://doi.org/10.1016/j.clsr.2020.105405

ties expect of data controllers and the sanctions for the non-compliance.

Gabriela Kennedy *(Partner), Mayer Brown (gabriela.kennedy@mayerbrown.com);*

Karen H.F. Lee *(Counsel), Mayer Brown (karen.hf.lee@mayerbrown.com).*

2. Hong Kong

2.1. *Artificial Intelligence: Guidelines Issued by HKMA*

On 1 and 5 November 2019, respectively, the Hong Kong Monetary Authority ("**HKMA**") issued a Circular on High-level Principles on Artificial Intelligence ("**Circular on AI Principles**") and a Circular on Consumer Protection in respect of Use of Big Data Analytics and Artificial Intelligence by Authorised Institutions ("**Circular on Customer Protection**").

The HKMA issued the Circulars after conducting a survey during the third quarter of 2019, which found widespread adoption of artificial intelligence ("**AI**") by banks in Hong Kong across all areas of their operations, from customer service chatbots to fraud and risk management.

2.1.1. *Circular on AI Principles*

The Circular on AI Principles was issued by the HKMA with the intent of providing guidance to banks on the design and adoption of AI. The guidelines are not intended to be stringent or prescriptive in nature, but to provide a balance between protecting consumers without hindering further technological developments. Banks are expected to take a risk-based approach when applying the principles, depending on the type of AI being adopted.

The Circular on AI Principles sets out 12 principles, which generally cover 3 areas – governance, application design and development, and ongoing monitoring and maintenance. In brief, these principles are as follows:

(a) **Board and senior management to remain accountable**
The board and senior management shall remain accountable for all automated and AI-driven decisions made by a bank. This brings into focus the importance of maintaining a clear governance framework and the deployment of risk management measures to ensure effective oversight over the use of AI within the bank.

(b) **Developers to have required competence**
Banks should only use personnel who have the necessary experience and competence to design and develop their AI applications. To achieve this, senior management must establish appropriate recruitment and training programmes, and implement supervisory mechanisms.

(c) **Ensure the AI application can be explained**
By implementing appropriate measures during the design phase, banks should ensure that their AI applications have an appropriate level of explainability taking into account the significance of each AI application deployed.

(d) **Using good quality data**
The data being used as part of the AI machine leaning must be relevant and of good quality, e.g. by carrying out data quality assessments within appropriately set metrics. Any issues that are discovered should be promptly escalated and rectified.

(e) **AI model validation**
Before any AI application is launched, extensive testing of the AI model must be carried out to confirm its accuracy and appropriateness (preferably this should be carried out by an independent third party).

(f) **Auditability**
Banks should maintain audit logs and relevant documentation for an appropriate period of time, to ensure that they can be used as evidence in the event of an investigation into an incident or unfavourable outcome in relation to the AI application.

(g) **Vendor oversight**
Due diligence should be carried out by the bank regarding any third party vendor used to develop the AI application, and management controls should be implemented to manage any risks.

(h) **Ethical, fair and transparent**
Measures must be implemented to ensure that any AI-driven decisions do not discriminate or unintentionally result in bias. The AI application must also be designed in a manner that complies with the bank's corporate values and ethical standards, and upholds consumer protection principles. Banks should be transparent with customers and clearly notify them if any service is powered by AI and the related risks.

(i) **Ongoing reviews and monitoring**
Banks should carry out periodic reviews and ongoing monitoring of the AI application to ensure that it still performs properly, in light of the fact that AI models may change due to their continued machine learning based on live data.

(j) **Comply with data protection requirements**
Effective data protection measures must be implemented by banks to ensure that any personal data collected and processed by the AI application complies with the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO"), and other applicable local and overseas regulatory requirements. Banks should use anonymised data to the extent possible.

(k) **Implement cybersecurity measures**
Banks need to ensure on an ongoing basis that their security measures are effective enough to handle new cyber threats that may be presented by the AI application.

(l) **Risk management and contingency plan**

Appropriate risk-management controls and contingency measures must be implemented, e.g. quality assurance checks, human intervention where necessary, ability to suspend the AI application and replace it with conventional processes if necessary, and so on.

The principles will be periodically reviewed and further guidance may be issued by the HKMA, from time to time.

2.1.2. *Circular on Customer Protection*

Along with the Circular on AI Principles, the HKMA issued the Circular on Consumer Protection to provide more specific guidance to banks on how to protect consumers in relation to the use of big data and AI in their operations. Whilst there is some overlap between the Circulars, the Circular on Consumer Protection provides more detail of what is expected of banks from a customer perspective. Similar to the Circular on AI Principles, banks should take a risk-based approach when applying the guidelines, depending on the type of big data and AI they use.

In summary, the Circular on Consumer Protection covers the following principles:

(a) **Governance and accountability**
The board and senior management must remain accountable for any decisions and processes driven by AI applications or big data. This includes ensuring that there is an appropriately documented governance, oversight and accountability framework in place; compliance with the consumer protection principles under the Code of Banking Practice, Treat Customers Fairly Charter and other relevant regulatory requirements; and validating the big data and AI applications prior to launch and on an ongoing basis, and so on.

(b) **Fairness**
Banks should ensure that big data and AI models result in objective, consistent, ethical and fair outcomes for customers. For example, ensuring that they comply with applicable laws regarding discrimination; that customers are not unjustifiably denied access to basic banking services; enabling manual intervention where necessary in order to mitigate any AI lending decision; taking customers' financial capabilities, situation and needs into account; and so on.

(c) **Transparency and disclosure**
Banks need to be appropriately transparent with customers regarding the use of big data and AI applications, and how they work. For example, they must clearly inform customers of the fact that a service will be powered by big data and AI technology and the risks involved; information should be provided to customers so that they can understand how their data is used by the AI; where requested by the customer, explain the type of data being used and what factors affect big data and AI-driven decisions (save that such explanations do not need to be provided for systems used to monitor and prevent frauds, money laundering or terrorist activities); implement a mechanism to enable customers to request a review on any decisions made by the big data and AI applications; and so on. The language used to communicate with the customer must be clear and simple (i.e. user friendly, and not too technical).

(d) **Data privacy and protection**
In addition to ensuring compliance with the PDPO and other relevant regulatory requirements, banks should also have due regard for the relevant guidelines issued by the Hong Kong Privacy Commissioner for Personal Data (e.g. Ethical Accountability Framework, Information Leaflet on Fintech, and so on). Further, banks are advised to take a privacy-by-design approach and to only collect and store the minimum amount of data necessary, for the shortest time possible. Where consent needs to be obtained in relation to the collection and use of personal data for any products or services to be provided by the bank, which are powered by big data and AI, banks need to obtain the consent in a clear and understandable manner to ensure that valid informed consent has been provided.

2.1.3. *Takeaway*

Whilst no one disputes the potential benefits of AI technology, many jurisdictions have started to become concerned with the associated risks – accountability, cybersecurity, ethics and bias, and consumer protection. Hong Kong is not the first country to issue guidelines to address some of these concerns. For example, in January 2019, the Singapore Personal Data Protection Commissioner issued a Proposed Model Artificial Intelligence Governance Framework, and in April 2019, the EU issued Ethics Guidelines for Trustworthy Artificial Intelligence (the first draft of which had been issued in December 2018).

Due to the broad nature of AI technology and their applicability, it is difficult to establish a one-size fits all regulation or policy. In order not to stifle innovation, but to also address the growing concerns regarding consumer protection, the regulators so far have taken a light approach, by providing guidelines and overarching principles to be taken into account by companies implementing AI technology.

As this area continues to develop, regulators globally will continue to pay close attention to the potential impact of AI, and we can expect to see more guidelines (and potentially mandatory regulations) issued in the future.

Gabriela Kennedy *(Partner), Mayer Brown (gabriela.kennedy@mayerbrown.com);*

Karen H.F. Lee *(Counsel), Mayer Brown (karen.hf.lee@mayerbrown.com).*

3. Australia

3.1. *Australia's privacy laws: Australian Government commits to considering and implementing widespread changes to privacy laws in response to regulator's report*

3.1.1. *Executive summary*

In response to a wide-reaching report on the operation of Digital Platforms in Australia (including a review and numerous recommendations for changes to Australia's privacy laws)

by the Australian Competition and Consumer Commission ("**ACCC**") last year, the Australian Government has accepted the need for reform and announced that it will consider a number of significant changes to Australia's privacy laws, subject to further consultation and review.

This article provides a high level summary of the key proposed changes and timelines that are being considered by the Australian Government.

3.1.2. *Background*

On 12 December 2019, the Australian Government released its response to the ACCC's final report for the Digital Platforms Inquiry ("**DPI Final Report**").

By way of background, the DPI was a broad-reaching inquiry into the impact of digital platforms – including search engines, social media and digital content aggregation platforms such as Google and Facebook – on competition in media and advertising services markets, undertaken by the ACCC in 2018-19.

The DPI Final Report made a number of recommendations across a breadth of policy areas, with some of the most significant aspects of the DPI Final Report relating to changes to Australia's privacy laws and strengthening consumer protection. These recommendations were largely economy-wide (with only one recommendation limited to digital platforms).

3.1.3. *Australian Government's Response*

The Australian Government has accepted the need for reform and largely supports the ACCC's recommendations, including in relation to reforms of Australia's privacy and data regulations. However, it is considering which recommendations it will actually implement, by when and to what extent.

Relevantly, in relation to privacy law reform, it is clear from the Government's response that Australia's privacy landscape is set to significantly change over the coming years, subject to further consideration and consultation.

Specifically, the Australian Government has stated that it will look to strengthen consumer protection under Australia's Privacy Act 1988 (Cth) ("**Privacy Act**") by:

(a) **Increasing penalties:** Increasing the penalties for breaches of the Privacy Act to the greater of (i) $10 million AUD; (ii) three times the value of the benefit obtained through the misuse of information; or (iii) 10% of the company's annual turnover.
(b) **Definition of personal information**: Amending the definition of personal information to capture technical data and other online identifiers (e.g. IP addresses, device identifiers, location data and any other online identifiers).
(c) **Strengthening existing notice and consent requirements**: For example, by requiring collection notices to be concise, transparent, intelligible and easily accessible, written in clear and plain language, and provided free of charge.
(d) **Introducing direct right of action**: Providing individuals with a direct right to bring actions to seek compensation for interferences with their privacy.
(e) **Binding code:** Developing a binding privacy code applicable to social media and other online platforms trading in personal information.

The Government has indicated that consultation and the subsequent introduction of draft legislation to Parliament to address the above reforms will occur in 2020.

The Government has also stated that it will undertake a comprehensive review of the Privacy Act in 2020, to be completed by 2021, which the Government has flagged will include consideration of the introduction of the right of erasure of personal information and a statutory tort for serious invasions of privacy.

3.1.4. *Detailed summary of key changes*

(a) **Increased penalties for breaches of the Privacy Act**

Currently, the maximum penalty for serious or repeated breaches of the Australian Privacy Act is $2.1 million. In March 2019, the Australian Government noted that this existing penalty "fall[s] short of community expectations, particularly as a result of the explosion in major social media and online platforms that trade in personal information".

Therefore, the Government has proposed to develop draft legislation to increase the maximum penalties for serious or repeated breached of the Privacy Act to the greater of:

(i) $10 million AUD;
(ii) three times the value of the benefit obtained through the misuse of information; or
(iii) 10% of the company's annual turnover.

The Government expects that the draft legislation will be released for public consultation and introduced to Parliament in 2020.

(b) **Definition of personal information**

The Australian Government has committed to amending the definition of 'personal information' in the Privacy Act to capture technical data and other online identifiers.

The Privacy Act currently defines personal information as "information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable".

In its DPI Final Report, the ACCC noted that in Australia there is significant legal uncertainty as to whether 'personal information' includes metadata such as IP addresses or other technical data. In light of "the volume of technical data relating to identifiable individuals that is collected, used and shared in digital markets", the ACCC recommended that the definition of 'personal information' be amended to capture technical information such as IP addresses, device identifiers, location data and any other online identifiers that relate to an identified individual. This amendment would reflect the wording used in the GDPR and further align Australia with international standards.

(c) **Notice and consent requirements**

The Australian Privacy Act currently requires entities to take "reasonable steps" to notify individuals in relation to the collection of personal information.

The Australian Government has committed to further consultation in relation to strengthening existing notice and consent requirements under the Privacy Act to ensure entities meet best practice standards, including by requiring entities to:

(i) provide "a notice of the information collected that is concise, transparent, intelligible and easily accessible, written in clear and plain language, and provided free of charge" that is "written at a level that can be readily understood by the minimum age of the child whose personal information is to be collected"; and

(ii) obtain consent whenever a "consumer's personal information is collected, used or disclosed" (unless certain exceptions apply, for example where the personal information is necessary for the performance of a contract to which the consumer is a party, or is required by law).

(d) **Direct right of action**

The Australian Government has also indicated that it will engage in further consultation in relation to introducing a direct right of action for individuals to bring actions in court to seek compensation for interferences with their privacy under the Privacy Act.

Limited avenues of redress are currently available to individuals for interferences with their privacy. In particular, individuals may only seek an injunction for breach of the Privacy Act or lodge a complaint with Australia's privacy regulator, the Office of the Information Commissioner ("OAIC"). Therefore, the ACCC recommended giving "individuals a direct right to bring actions and class actions against APP entities to seek compensation for an interference with their privacy". This would further align Australian privacy law with international standards, including the UK, New Zealand, and the EU.

(e) **Binding privacy code**

Finally, the Australian Government (as previously stated in March 2019) will also amend the Privacy Act to require the OAIC to develop an enforceable Privacy Code of Practice that applies to digital platforms.

The code will provide specific rules protecting the personal information of children and vulnerable groups, and require entities to, among other things, be more transparent about data sharing, meet best practice consent requirements when collecting, using and disclosing personal information, and stop using or disclosing personal information upon request.

(f) **Comprehensive Privacy Act review**

More generally, the Australian Government has stated it will undertake a comprehensive review of the Privacy Act, including considering whether to introduce a right of erasure for consumers, throughout 2020-21.

In summary, the Government's response indicates that Australia's privacy landscape is set to significantly change over the coming years. However, it appears that there will be significant opportunity for stakeholders to engage with the Government and regulators on the substance and form of these changes.

Philip Catania *(Partner), Corrs Chambers Westgarth, (Philip.Catania@corrs.com.au);*

Georgia Westbrook *(Lawyer), Corrs Chambers Westgarth, (Georgia.Westbrook@corrs.com.au);*

Rachael Pluta *(Lawyer), Corrs Chambers Westgarth, (Rachael.Pluta@corrs.com.au).*

4. Japan

4.1. *Administrative advisory to Recruit Carrier for selling student job hunters' data without consent*

4.1.4. *Introduction*

The Personal Information Protection Committee ("**PIPC**") of the Japanese Government has found Recruit Carrier Co., Ltd. ("**Recruit Carrier**") in violation of the Personal Information Protection Act ("**PIPA**") by illegally selling data regarding the probability of students declining informal job offers from companies and issued administrative advisories to Recruit Carrier on 26 August and 4 December 2019.

4.1.5. *Summary of case*

Recruit Carrier is a Japanese company which operates a recruitment information site, "Rikunabi". By registering as a member of Rikunabi, candidates can review various companies' recruiting information and submit job applications to these companies through Rikunabi. Rikunabi is a major recruitment information site in Japan with a large number of student memberships and exclusive recruiting arrangements with several companies.

In March 2018, Recruit Carrier started a service providing information to companies recruiting students relating to the probability of each student declining informal job offers made from the company ("**Service**"). Using information from a list of students who declined informal job offers in the previous year (i.e. 2017), the Service predicted the probability of students declining informal job offers in 2018 based on those students' browsing histories by using artificial intelligence.

Prior to March 2019, Recruit Carrier collected data including IDs of assigned students and cookie data from their client companies, although such data did not include the students' names. Recruit Carrier then predicted the probability of these students declining informal job offers based on their browsing histories of Rikunabi and other websites which had been obtained through the cookie data collected. Based on the cookie data, where students review both the company's website and Rikunabi under the same browser, it would have been possible to presume that the person who had reviewed the company's website would be the same person who had reviewed Rikunabi. Recruit Carrier would provide the prediction data together with the student's ID to the companies and these companies then used the prediction data by matching it to the student's ID and name. Recruit Carrier did not obtain consent from students for providing such data to the companies.

After March 2019, Recruit Carrier revised its privacy policy, under which it would obtain consent from newly registered student members for providing their personal information data to the companies. However, Recruit Carrier did not obtain consents from approximately 8,000 students who had already registered for membership prior to March 2019 and these students were not given the opportunity to provide their consents through the Rikunabi site.

Recruit Carrier later suspended the Service in July 2019, in response to the PIPC's comments, and eventually abolished the Service on 4 August 2019.

4.1.6. Administrative advisory

(a) **Administrative Advisory on 26 August 2019**

On 26 August 2019, the PIPC held that the Service provided after March 2019 had violated the PIPA since Recruit Carrier had processed personal information such as students' names for the purpose of analyzing the probability of declining job offers and provided the prediction data of 8,000 students to companies without obtaining consents from these students. Consequently, an administrative advisory was issued to Recruit Carrier.

Under the PIPA, where the PIPC recognizes a need for protecting an individual's rights and interests in cases where an entity handling personal information has violated certain provisions of the PIPA, the PIPC may issue an administrative advisory to request such entity to suspend the violating act or take other necessary action to rectify the violation. The administrative advisory to Recruit Carrier was the first one ever issued by the PIPC since its establishment in January 2016.

However, the administrative advisory issued on 26 August 2019 did not address the Service provided before March 2019. Under the PIPA, 'personal information' is defined as information that is able to identify a specific individual, such as name, date of birth, or other descriptions, including those which can be readily collated with other information and thereby identify a specific individual. It was generally considered that cookie data itself does not fall into "personal information." The PIPC also shared the following views regarding cookies: "If cookie data is linked to member information and can identify a specific individual, it must be treated as personal information under the PIPA", but "cookie itself is a widely used technology including session management as an identifier and its usage characteristics are diverse. Therefore, in addition to the provisions of the current Act, careful consideration should be given to the need to regulate cookies individually."

(b) **Administrative Advisory on 4 December 2019**

On 4 December 2019, the PIPC held that the Service provided before March 2019 also violated the PIPA since (i) Recruit Carrier knew that the companies receiving the IDs and the probability data for declining the job offers were able to identify each specific individual; (ii) Recruit Carrier avoided obtaining consents from students for providing such data to the companies based on the reasoning that Recruit Carrier could not identify a specific individual solely from the cookie data, and (iii) Recruit Carrier provided an extremely inappropriate service that violated the spirit of the law. The PIPC issued an administrative advisory to Recruit Carrier and Recruit Co., Ltd. (the parent company of Recruit Carrier) requesting them to take the necessary measures to protect personal rights and interests appropriately. The PIPC also issued an administrative guidance to 35 companies who had received the prediction data from Recruit Carrier, including Toyota Motor Corporation, Kyocera Corporation and Mitsubishi Corporation.

4.1.7. Impact

On 6 September 2019, the Ministry of Health, Labour and Welfare ("**MHLW**") issued an administrative guidance to Recruit Carrier stating that the Service may be in violation of the Employment Security Act whichi prohibits the provision of personal information to third parties without a special reason, regardless whether individual consents were obtained or not. The MHLW also considered the fact that students would be forced to give their consents considering that many students were using Rikunabi.

On 29 November 2019, the PIPC published a summary of the revised bill of the PIPA. is the summary stated that regulations restricting the provision of personal data to third parties shall apply to information that does not constitute personal data under the possession of the provider, but clearly constitutes personal data when received by entities from the data provider. In this summary the case of Recruit Carrier was considered. The PIPC also stated that cookies, ID or passwords for logging into a company's website may constitute such information that will be restricted under the revised PIPA. The PIPC plans to submit the revised bill to the parliament in 2020.

Kiyoko Nakaoka *(Partner), KUBOTA, (nakaoka@kubota-law.com).*

5. Malaysia

5.1. 5G *in Malaysia today*

Self-driving cars, remotely controlled robot surgeons, lifelike holograms – the stuff of sci-fi – will soon become reality with 5G. Asimov would be proud. 5G has been a consistent headliner in 2019 despite a fast-evolving world, and 2020 will be no different. But what is 5G?

The term 5G merely denotes the fifth generation of mobile network with the 'G' in 5G being an abbreviation for 'generation'. There is no universal definition for 5G but it is perhaps more precise to explain 5G as a combination of several key technologies with the objective to achieve faster speed, lower latency and the ability to simultaneously connect devices on a massive scale.

5.1.4. Key technologies of 5G

Radio frequencies form the foundation of mobile network technology but the radio spectrum is finite and cannot be expanded despite increasing use of the same. Thus, the solution to this problem as part of 5G implementation is to use millimetre waves, sometimes defined to lie above 24 gigahertz (tradi-

tional mobile frequencies are below 6 gigahertz), in addition to lower frequencies.

Traditionally, millimetre waves are not considered ideal for mobile services because of their inability to travel through obstacles easily. However, the new approach involves the use of millimetre wave frequencies to connect mobile users to nearby base stations, and this is where a new technology known as small cells comes into play. Using these small cells as part of the Radio Access Network will allow the millimetre waves to travel more effectively. A popular idea is to install these small cells on existing structures such as lampposts which will allow them to be effectively distributed in clusters. However, the lower frequencies will still remain crucial as they allow for a broader coverage due to its longer wavelength, which will be necessary for massive IoT usage. As such, the implementation of 5G will likely require a combined usage of the low, mid and high frequency bandwidths.

The other key feature of 5G implementation is the 'massive' multiple input, multiple output ("**MIMO**") antennas which will allow more users to simultaneously connect to the network. Combined with beamforming technology, massive MIMO will allow the antennas to focus the signal to the particular user or device which will ultimately increase efficiency and reduce wastage of the signal.

5.1.5. *5G implementation efforts in Malaysia*

The implementation of 5G would be in line with Malaysia's National Fiberisation and Connectivity Plan (NFCP) 2019-2023 which was formulated to, among others, improve broadband quality and Internet access for all Malaysians. In November 2018, the Malaysian Communications and Multimedia Commission ("**MCMC**"), which is the telecommunications regulator in Malaysia, established a national 5G Task Force comprising both public and private sector members with the objective of studying and recommending the strategies for 5G deployment in Malaysia. The Task Force is divided into four main working groups focusing on different areas, namely: (i) business case; (ii) infrastructure; (iii) spectrum management and allocation; and (iv) regulatory.

In October 2019, MCMC announced that 5G demonstration projects will commence across six states (Kedah, Kuala Lumpur, Penang, Perak, Selangor and Terengganu) in Malaysia for a period of six months. In collaboration with private corporations, the use cases that will be tested during the six months include smart traffic lights, smart parking, smart agriculture and augmented reality ("**AR**") for education. According to MCMC's Chairman, the 5G utilisation test cases in Langkawi in Kedah in the agriculture, digital healthcare, education, smart city, smart transportation and tourism sectors have been impressive with around 37 cases of utilisation in just two months of implementation.

Spectrum is the heart and core of any 5G rollout. Hence, on 31 December 2019, MCMC took the first crucial step in identifying the 700MHz band, 3.4GHz to 3.6 GHz ("**3.5 GHz band**") and 24.9GHz to 28.1GHz ("**26/28 GHz band**") as the pioneer spectrum bands for the 5G roll-out in Malaysia in its final report on the 'Allocation of spectrum bands for mobile broadband service in Malaysia' ("**Final Report**"). The Final Report describes amongst others the award mechanism for the allocation of spectrum bands which is expected to commence in the first quarter of 2020. This award mechanism has been briefly summarised below:

(a) For the 700 MHz and 3.5 GHz bands, MCMC is considering allocating these bands to a single entity comprising a consortium formed by multiple licensees instead of an individual licensee to encourage a cost-efficient collaboration between operators by avoiding duplication of infrastructure. Currently, the main mobile telecommunications service providers in Malaysia are Maxis, Celcom Axiata, Telekom Malaysia (webe), Digi, U Mobile and YTL (Yes4G). The 700 MHz and 3.5 GHz bands will be assigned in one package through a tender process (beauty contest). As this is a new approach, MCMC will only make available 2×30 MHz of the 700 MHz band and 100 MHZ of the 3.5 GHz band in the first stage. More information will be available for interested parties when MCMC releases the applicant information package (AIP). The remaining frequencies of these bands will be considered for assignment at a later stage.
(b) The 26/28 GHz band will be assigned in two ways:
    (i) For the 24.9GHz to 26.5GHZ bands, these will be assigned through a tender process (beauty contest) to licensees. However, parties that have successfully been assigned with this frequency range will not be eligible to apply for the 26.5GHz to 28.1GHz bands;
    (ii) For the 26.5GHz to 28.1GHz bands, these will be assigned on a first-come first-served basis and will be open to any party (including non-licensees) for the purpose of deploying localised and/or private networks. MCMC will issue a notice on the start date to allow for the submission of the AA application.

The assignment of the pioneer spectrum bands will be conducted by way of an Apparatus Assignment ("**AA**"), which MCMC anticipates to be more economical in terms of spectrum fees, thus encouraging network deployment by service provider(s). Cost savings can then be passed on to businesses and consumers.

The identified spectrum bands offer a balance between the wide coverage of lower frequencies (through the 3.5 GHz band) and high capacity of the millimetre-wave spectrum (through the 26/28 GHz bands, which support large bandwidths and high data rates, making them ideal for increasing the capacity of wireless networks). Once the assignment of the spectrum bands is completed, MCMC expects the commercial deployment of 5G in Malaysia to begin in the third quarter of 2020.

According to the MCM, the existing allocation for 4G will be maintained, which includes maintaining the existing allocation of the 2300MHz and 2600MHz bands until December 2021 in parallel with the necessary preparation for migration towards 5G.

5.3.6. *What next?*

Like elsewhere in the world, there is still much to be considered technically and legally in implementing 5G but in Malaysia, there are expectations that the commercial deployment of 5G will begin in the third quarter of 2020 with in-

evitable changes to our regulatory framework. Therefore, anyone seeking to be a part of the 5G ecosystem (whether as part of implementation of 5G or through the application of 5G) in Malaysia must remain on their toes and ensure compliance with the laws and regulations which are expected to change over the next few years.

Natalie Lim *(Partner), Skrine (natalie.lim@skrine.com);*
Lam Rui Rong *(Associate), Skrine (lam.rui.rong@skrine.com).*

6. Singapore

6.1. *PDPC publishes new chapter on Cloud Services*

On 9 October 2019, the Personal Data Protection Commission ("**PDPC**") has introduced a new chapter 8 on "Cloud Services" in the Advisory Guidelines on PDPA for Selected Topics (" **Guidelines**"), so as to provide clarity on the responsibilities of organisations using cloud services to process personal data in the cloud, as well as the responsibilities of cloud service providers (" **CSPs**") when processing personal data on behalf and for the purposes of organisations.

6.1.1. *Key features of new Guidelines*

(a) **CSP's Processing of Personal Data.** The PDPC clarified that a CSP which processes personal data for another organisation is considered a data intermediary and would be subject to PDPA obligations applied to data intermediaries, namely:
   (i) the Protection Obligation which requires the CSP to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and
   (ii) the Retention Limitation Obligation which requires the CSP to cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that: (1) the purpose for which that personal data was collected is no longer being served by retention of the personal data; and (2) retention is no longer necessary for legal or business purposes.

(b) **Organisations' Responsibilities.** The PDPC had also clarified that when using cloud services, the organisation is responsible for complying with all obligations under the Personal Data Protection Act 2012 ("**PDPA**") in respect of personal data processed by the CSP on its behalf and for its purposes, as the CSP is treated as an intermediary.

(c) **Overseas Transfer of Personal Data.** Under Section 26 of the PDPA, an organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under the PDPA (the "**Transfer Limitation Obligation**").
In this regard, the PDPC clarified that where an organisation engages a data intermediary to process personal data on its behalf and for its purposes, the organisation (and not the data intermediary) is responsible for complying with the Transfer Limitation Obligation in respect of any overseas transfer of personal data. This is regardless of whether the personal data is transferred by the organisation to an overseas data intermediary, or transferred overseas by the data intermediary in Singapore as part of its processing on behalf and for the purposes of the organisation.
In particular,
   (i) the organisation may be considered to have taken appropriate measures to comply with the Transfer Limitation Obligation by ensuring that personal data may only be transferred to overseas locations with comparable data protection laws, or that the recipients (e.g. data centres or subprocessors) in these locations are legally bound by similar contractual standards; and
   (ii) where the contract between an organisation and its CSP does not specify the locations to which a CSP may transfer the personal data processed and leaves it to the discretion of the CSP, the organisation may be considered to have taken appropriate steps to comply with the Transfer Limitation Obligation by ensuring that:
      (1) the CSP based in Singapore is certified or accredited as meeting relevant industry standards (eg. such as ISO27001 and Tier 3 of the Multi-Tiered Cloud Security/MTCS certification); and
      (2) the CSP provides assurances that all the data centres or subprocessors in overseas locations that the personal data is transferred to comply with these standards, and can produce for example technical audit reports such as the SOC-2 upon request.

6.1.5. *Comment*

Given the increased use of cloud services by organisations, the PDPC's latest updates provide good guidance for organisations in understanding the scope of their responsibilities under the PDPA.

6.2. *Issuance of Codes of Practice under the Protection from Online Falsehoods and Manipulation Act*

In exercise of the powers conferred by Section 48 of the Protection from Online Falsehoods and Manipulation Act 2019 (No. 18 of 2019) ("**POFMA**"), the newly established Protection from Online Falsehoods and Manipulation Act Office in the Infocommunications Media Development Authority ("**POFMA Office**") had issued three Codes of Practice which came into operation on 2 October 2019:

(a) Code of Practice for Giving Prominence to Credible Online Sources of Information ("**Prominence Code**");

(b) Code of Practice for Transparency of Online Political Advertisements ("**Political Advertisements Code**"); and
(c) Code of Practice for Preventing and Countering Abuse of Online Accounts ("**Online Accounts Code**").

These Codes of Practice seek to ensure that the prescribed internet intermediaries and digital advertising intermediaries have adequate systems and processes in place to prevent and counter the misuse of online accounts by malicious actors, enhance the transparency of political advertising, and deprioritise online falsehoods.

6.2.5. Prominence Code.

The Prominence Code sets out the obligations that prescribed internet intermediaries have to comply with so as to give prominence to credible online sources of information and/or not give prominence to a declared online location under POFMA, any material included on an online location that is or that contains a false statement of fact that is the subject of a Part 3 Direction (i.e. a "Correction Direction" or a "Stop Communication Direction") or Part 4 Direction (i.e. a "Targeted Correction Direction", a "Disabling Direction" or a "General Correction Direction") under POFMA (collectively, the "**POFMA Directions**"), or any material that is the subject of the POFMA Directions.

In particular, prescribed internet intermediaries must, inter alia, (1) put in place reasonable due diligence measures so as to achieve the above purposes; and (2) provide the POFMA Office with an annual report on the implementation of such due diligence measures. Such due diligence measures include, inter alia:

(a) prioritising relevant and authoritative information and increasing the visibility of such information where appropriate in automatically ranked distribution channels, or reducing the visibility of material subject to the POFMA Directions;
(b) providing contextual information to sources of relevant and authoritative information where available; and
(c) ensuring that declared online locations under POFMA and materials subject to POFMA directions do not appear in sections meant to promote viewership.

6.2.6. Political Advertisements Code

The Political Advertisements Code and its annexes set out the obligations that prescribed digital advertising intermediaries and internet intermediaries have to comply with to enhance transparency of online political advertisements.

In particular, prescribed digital advertising intermediaries and internet intermediaries must, inter alia, (1) put in place reasonable due diligence measures to enhance the disclosure of information concerning any online political advertisement that is communicated in Singapore; and (2) provide the POFMA Office with an annual report on the implementation of such due diligence measures. Such due diligence measures include, inter alia:

(a) verifying the eligibility of advertisers for political advertisements pertaining to elections in Singapore;
(b) ensuring that online political advertisements are accompanied with easily accessible disclosure notices containing the name of person(s) or organisation(s) that requested to place or paid for the advertisement;
(c) maintaining and making available for viewing by the POFMA Office a record of all such online political advertisements; and
(d) developing techniques to identify and flag online political advertisements targeted at end-users in Singapore that are undisclosed, miscategorised, or placed by unverified persons or organisations.

6.2.7. Online Accounts Code

The Online Accounts Code and its annexes set out the obligations that prescribed internet intermediaries have to comply with in preventing and countering the abuse of online accounts.

In particular, prescribed internet intermediaries shall, inter alia, (1) put in place reasonable due diligence measures to (I) safeguard against misrepresentation of the identity of an end-user; (II) ensure that bots' activities are not confused with human interactions; and (III) limit abuse of their platforms through the use of inauthentic online accounts; and (2) provide POFMA Office with an annual report on the implementation of such due diligence measures. Such due diligence measures include, inter alia:

(a) having a published policy that prohibits the misrepresentation of identity and states what constitutes impermissible use of bots;
(b) having reasonable verification measures in place to prevent the creation and usage of unauthentic accounts or bots for malicious activities;
(c) verify account and/or pages belonging to political parties and candidates during election periods; and
(d) requiring the holder of any online account that employs a bot to communicate or interact with end-users to effectively disclose the use of the bot(s).

6.2.8. Comment

These Codes of Practice set out up-stream measures that prescribed intermediaries, such as social media platforms, must implement to prevent their platforms from being used to spread falsehoods; prevent and counter the misuse of online accounts by malicious actors who can hide behind them by being anonymous; enhance the transparency of political advertising; and downplay online falsehoods. Together with the existing POFMA framework, it provides the Government with multiple avenues to tackle growing concerns over fake news and misinformation, communicated particularly through various online and social media platforms.

Lam Chung Nian *(Partner), WongPartnership LLP (chungnian.lam@wongpartnership.com);*

Kenji Lee *(Associate), WongPartnership LLP (kenji.lee@wongpartnership.com).*

7. South Korea

7.2. *Major Amendment to the Personal Information Protection Act Passed by National Assembly*

On January 9, 2020, amendments to Korea's 3 major data privacy laws ("**Three Data Laws**"), i.e., Personal Information Protection Act ("**PIPA**"), Act on the Promotion of Information and Communications Network Utilization and Information Protection ("**Network Act**"), and Credit Information Use and Protection Act ("**Credit Information Act**"), were passed at a plenary session of the National Assembly of Korea.

We live in an era of data-driven economy where the use of new technologies such as artificial intelligence (AI), cloud services, and Internet of Things (IOT) have become a necessity in order to process increasingly larger amounts of data and develop new businesses in the IT sector. In line with the legislative trends in other major parts of the world, there has long been a push in Korea towards amending the Three Data Laws to ensure the secure use of personal information while still paving the way for the more efficient processing of big data. The revisions to the Three Data Laws are the culmination of such efforts.

The amendments to the PIPA that have been adopted include, among others: (i) clarification of the definition of "personal information," (ii) the introduction of pseudonymized information and the permitted use of pseudonymized information for research and statistical purposes without the data subject's consent, (iii) the introduction of compatibility, (iv) the transfer of the Network Act's personal information-related provisions to the PIPA and (v) elevation of the Personal Information Protection Commission's ("**PIPC's**") status to a central administrative agency responsible for the enforcement of the PIPA.

Given the importance of the newly amended PIPA and its potential implications on data-reliant industries regulated by the PIPA, we have summarized below the key changes to the law.

7.2.4. *Key Provisions of the Amended PIPA*

(a) **Clarification of the definition of "personal information" (Article 2(1))**

As is the case under the current PIPA, the definition of "personal information" under the amended PIPA continues to include "information that can be easily combined with any other information to identify a specific individual." The amended PIPA provides clearer direction on what this means by stipulating the criteria for determining whether certain information can be "easily combined with any other information to identify a specific individual." The specific criteria set forth in the amended PIPA is that one must give "reasonable consideration to factors such as time, cost, and technology required for identifying an individual, including the likelihood of obtaining additional information to be combined with the subject information." The above criteria is intended to prevent the definition of personal information from being interpreted too broadly under the PIPA.

(b) **Introduction of "pseudonymized information" (Article 2(1)(c), 2(1-2), 2(1-8) and Chapter 3)**

The amended PIPA introduces the concept of "pseudonymized information," which means "information which, through the process of pseudonymization, may no longer be used to identify a specific individual without using or combining additional information to restore the information to its original state." Here, "pseudonymization" means the process of fully or partially deleting or replacing personal information or employing other similar methods such that the personal information can no longer be attributed to a specific individual without additional information.

The initial draft amendment of the PIPA that was proposed to the National Assembly by Representative Jae-Geun IN ("Initial PIPA Bill") provided that the specific methods of pseudonymization would be set forth in the relevant Presidential Decree. However, the final version of the amendment which passed the National Assembly stipulates the principles governing the pseudonymization methods in the PIPA itself, rather than delegating the authority to the President to determine such methods in the Presidential Decree. Therefore, data handlers are advised to continue monitoring the position of the pertinent regulators, including any guidelines to be issued by them, and see how the principles stipulated in the amended PIPA will be applied in practice going forward.

Under the amended PIPA, data handlers may process pseudonymized information without the consent of the data subject for purposes including statistical compiling, scientific research, and record preservation for the public interest. Moreover, the PIPA's provisions regarding the destruction of personal information and the data subject's right to request access, or the correction/deletion of personal information, do not apply to pseudonymized information. As stated in the reasons for the proposed amendment to the PIPA, "scientific research" purposes include "commercial purposes such as the development of data-based, innovative technology, products, and services." The wider scope of purposes for which personal information may be used and provided to third parties under the amended PIPA is in line with the demands of the current data economy.

Meanwhile, the amended PIPA regulates the combining of pseudonymized information managed by different data handlers by stipulating that only professional institutions designated by the PIPC or by the head of a pertinent central administrative agency may combine such pseudonymized information. Also, the combined information may only be exported outside of the professional institution after obtaining the approval of the head of the said institution.

Furthermore, the amended PIPA requires that anyone who processes pseudonymized information must implement the statutorily-prescribed security measures. Processing pseudonymized information for the purpose of identifying a specific individual is also prohibited under the amended PIPA. Anyone who violates this prohibition may be subject to a penalty surcharge of 3% or

less of their total revenue, and imprisonment of up to 5 years or a fine of up to KRW 50 million.

(c) **Use of personal information within the scope reasonably related to the original purpose of the collection (Article 15(3), Article 17(4))**
The amended PIPA allows data handlers to use or provide personal information within the scope reasonably related to the original purpose of the collection without the consent of the data subject in accordance with the Presidential Decree to be promulgated, after considering, for example, whether such use or provision may result in any disadvantage to the data subject and/or whether the data handler has implemented the necessary safeguards to ensure the security of the personal information, e.g., encryption. By doing so, the amended PIPA has relaxed the existing consent-oriented regulations which have been subject to continued criticism for being excessively formalistic and stringent and adopted the purpose limitation principle of the GDPR, which allows the use of personal information for purposes that are not incompatible with the purpose of initial collection. The specific details regarding the method of using and providing personal information for the purposes as described above will be set forth in the Presidential Decree, so it is important to continue monitoring any amendments to be made to the Presidential Decree.

(d) **Exclusion of anonymized information from the application of the PIPA (Article 58(2))**
The amended PIPA explicitly provides that any information which cannot be used to identify a specific individual even if the information is combined with any other information, after reasonably considering factors such as time, cost, technology ("Anonymized Information"), is not subject to the provisions of the PIPA.
Under the current PIPA, Anonymized Information is already considered as non-personal information which is not subject to the PIPA. However, to avoid any dispute over potential gray areas, the amended PIPA explicitly states that Anonymized Information is excluded from the application of the PIPA.

(e) **Transfer of the Network Act's personal information-related provisions to the PIPA (Chapter 6)**
The amended PIPA includes a new chapter on the "Special Provisions for the Processing of Personal Information by Information and Communications Service Providers and Recipients of Personal Information Provided by Information and Communications Service Providers (collectively, the "ICSPs")" ("Special Provisions"), which basically consists of the Network Act's provisions relating to personal information protection that are not in harmony with those set forth in the PIPA. Examples of such provisions include those on the collection and use of personal information, notification and report of personal information leakages, destruction of personal information of inactive users, notification of personal information usage details/records, damage compensation guarantees, designation of a domestic representative, protection of personal information transferred abroad, and penalty surcharges.

(f) **Consent no longer required for an ICSP's outsourcing of data processing to a third party**
Under Article 25 of the current Network Act, an ICSP who wishes to outsource the processing of personal information to a third party ("Outsourcing") is obligated, in principle, to obtain the data subject's (i.e., user's) consent. However, this provision was not transferred to the amended PIPA as part of the Special Provisions, and thus the PIPA's provisions on Outsourcing will now apply to an ICSP who wishes to engage in Outsourcing.
Under the current PIPA, the data subject's consent is not required for Outsourcing. However, because the Network Act included such a consent requirement, ICSPs were required to obtain separate consent to not just the collection/use of personal information and provision of personal information to a third party, but also Outsourcing. Due to this additional consent requirement, Article 25 of the Network Act was often mentioned as one of the main reasons that IT service providers were prevented from more actively utilizing cloud services, which is generally how most IT service providers process data of their customers.
The Initial PIPA Bill included Article 25 of the Network Act as one of the Special Provisions to be transferred to the PIPA. Yet, the idea of transferring Article 25 to the PIPA was discarded during the bill review process after several legal and industry experts pointed out the problems with doing so and data handlers/ICSPs also criticized the possible implications.

(g) **Streamlining of Korea's data protection regulatory authorities (Article 7, 7-14)**
The PIPC will be elevated to a central administrative agency reporting to the Prime Minister, and also become the supervisory authority for data breaches (including the misuse/abuse of personal information and leakages). Personal information protection matters that are currently handled by multiple agencies (i.e., Ministry of Public Administration and Security, Korea Communications Commission) will all be handled by the PIPC instead. In order to ensure the independence of the PIPC, Article 18 of the Government Organization Act – which stipulates the Prime Minister's authority to direct and supervise the heads of central administrative agencies under orders from the President, and revoke or suspend any administrative orders issued by the head of a central administrative agency if they are deemed unlawful or unjust – will not apply to certain tasks performed by the PIPC.

7.2.5. Amended Network Act: deletion of personal information-related provisions

As explained above, in order to achieve harmonization among the Three Data Laws, the personal information-related provisions of the Network Act have been transferred to the PIPA, and thus the said provisions (i.e., Chapter 4 (Protection of Personal Information)) have been deleted from the Network Act.

7.2.6. Amendments to the Credit Information Act and Act on the Protection and Use of Location Information

The amendment to the Credit Information Act was also passed by the National Assembly's plenary session on January 9, 2020 - the same date that the amendments to the PIPA and Network Act were passed. Among the changes that were adopted, certain provisions of the Credit Information Act that overlapped with the PIPA were revamped so that the relevant provisions of the PIPA would apply instead, and some provisions were revised to clarify the Credit Information Act's relationship with the PIPA. As such, in order to determine whether the amended PIPA (and not the Credit Information Act) will apply to the processing of an individual's personal credit information, concerned businesses and companies should review the PIPA's new changes in detail. For your information, the amended Credit Information Act stipulates that the PIPC has the authority to supervise personal credit information that is processed by a business operator and not a financial institution, while the Financial Services Commission has supervisory authority over personal credit information processed by financial institutions.

The draft amendment for the Act on the Protection and Use of Location Information ("**Location Information Act**") - which was also proposed to the National Assembly on November 15, 2018 along with the draft amendments of the PIPA and Network Act – includes a provision that would transfer the KCC's authority to enforce/oversee matters relating to the protection of personal location information (which qualifies as personal information) to the PIPC, and have the KCC and PIPC be jointly responsible for enforcing the Location Information Act. The National Assembly's review of the Location Information Act's amendment bill has been postponed due to the need to further discuss and clarify the respective scope of tasks to be performed by each of the two authorities. As such, it would be helpful to keep an eye on whether the bill is eventually passed.

The new PIPA is meaningful in that it provides clearer guidance to data handlers on what constitutes the lawful processing of personal information and also sets forth the standards for the secure processing of personal information. Yet, since the amended PIPA also imposes additional obligations on data handlers and provides for heavier sanctions (e.g., introduction of a penalty surcharge) in the case of a violation, the recent changes should not be taken lightly.

The amended PIPA is expected to go into effect 6 months from its promulgation date, and the amendment of the PIPA's implementing regulations and related public notices are also expected to take place in the upcoming months. Therefore, we recommend that anyone who is likely to be affected by the new PIPA review the changes carefully and continue to monitor any related legislative developments.

Kwang Bae Park *(Partner), Lee & Ko (kwangbae.park@leeko.com)*

8. Thailand

8.2. *Thailand's Digital Law Landscape Update 2020*

Over the past two years, the Thailand government has moved aggressively forward on its new Digital Economy policy platform, also known as "Thailand 4.0". This included a raft of new laws that were drafted, enacted and implemented in this relatively short period which saw significant changes to legal areas such as cybercrimes, e-commerce, data privacy, digital taxation, cryptocurrency, fintech and others.

8.2.4. Ministry Restructure

The government launched Thailand 4.0 by enacting the Digital Economy Promotion Act which took effect in January 2017. Under this act, the Ministry of Information and Communication Technology ("**MICT**") was replaced with the new Ministry of Digital Economy and Society ("**MDES**"). The MDES will have the same purview of government agencies as did the MICT, but will also include oversight of the new Digital Economy and Society Committee which has been tasked with setting new policy and guidelines under Thailand 4.0, as well as the newly formed Government Committee for Cyber-Security under the proposed Cybersecurity Act and the newly revised Computer Crimes Act, with both committees to be chaired by the Prime Minister.

8.2.5. E-Commerce and Payment Systems

The amendments to the Electronic Transactions Act expanded the binding effect of digital communications in transactions and as evidence In particular, they included "automated" electronic communications as binding notwithstanding the absence of human involvement even in the case of two automated systems communicating with each other, effectively recognizing the new "Internet of Things" communications.

The earlier Royal Decree on E-Payment and other patchwork laws and regulations, which were implemented over the past ten years to address the disruption of non-traditional payment, was replaced by the new Payment Systems Act in 2017 (the "**PSA**"), with legal regulations enacted in 2018 to address all current "electronic payment systems" and "electronic payment services" as well as all future/experimental technologies under one administrative body of law to be overseen by the Bank of Thailand.

This new PSA has resulted in the mandatory licensing or registration of payment systems or payment services including not only the traditional credit, debit, ATM cards and other money transfer businesses, but also new technologies represented by payment facilitators and electronic money services utilizing pre-paid, stored-value online accounts.

However, the PSA affords sufficient exemptions to licensing/registration for new and smaller operators to avoid stifling innovation and enable the expansive use of digital currency with the publicly-announced goal of having Thailand become a cashless society.

The government has also actively promoted its own PromptPay cashless payment system through the Bank of Thailand which is linked to the identification of Thai citizens, as well as establishing a standardized QR Code system utilized by many operators to facilitate payments through PromptPay.

8.2.6. Cryptocurrency, Digital Tokens and ICOs

The past two years have seen new laws being enacted to encourage digital token operators in Thailand by creating a more

transparent framework for operations and public investment under government auspices. The Royal Decree on Digital Assets Business ("**Royal Decree**") has broken down the definitions "cryptocurrency" and "digital tokens" into new definitions based on respective functions. The Royal Decree implements a licensing regime for all "Digital Asset Businesses" ("**DABs**") including DAB exchanges, brokers and dealers. The Royal Decree also authorizes the Securities and Exchange Commission ("**SEC**") to recognize new DAB operations as and when appropriate.

Since 2018, the SEC has also enacted a series of implementing regulations addressing digital token offerings to the public. Funding through any kind of public offering of digital token (i.e. all ICOs) must be considered and approved by the SEC under the new Royal Decree and can only be accomplished through a digital token system provider (ICO Portal) approved by the SEC. The SEC also continues to maintain oversight post-ICO to protect digital asset investors and ensure balanced protection.

There has also been a contemporaneous Amendment to the Revenue Code (No. 19) which includes revenue from digital assets as taxable income and subjects such revenue to withholding tax at the rate of 15 percent.

Assessable income from digital assets includes:

(a) Share of profits or other similar benefits obtained from holding or possessing a digital token; and
(b) Benefits from digital asset transfers, in which only the valuation is made in excess of the investment amount.

8.2.7. Financing Technologies (FinTech)

In 2018, Thailand hosted a government-sponsored Bangkok FinTech Fair which was the first of its kind in Thailand, and was recently followed in July, 2019 by its second iteration. The government has indicated a strong interest in pursuing new business in this area as part of its Thailand 4.0 digital economy. However, Thailand has traditionally been more conservative in its oversight of public financing and the government has shown similar cautiousness here.

However, to encourage new FinTech technologies, both the Bank of Thailand and the Thai SEC had initiated a regulatory "sandbox" for interested operators in this area for the past several years. This provides operators with a safe environment for testing FinTech products and services while cooperating with the BOT and SEC to develop future regulations.

Since that time, the BOT enacted its 2019 Notification 4/2562 Re: The Determination of Rules, Procedures, and Conditions for Peer-to-Peer (P2P) Lending Businesses and Platforms ("**BOT P2P Notification**"). This BOT Notification now establishes guidelines for P2P lenders, borrowers and P2P platform providers. It defines certain types of P2P businesses, establishes minimum requirements for their establishment, and sets limitations on such operations (e.g. maximum loan amounts, interest rates, etc.). While it has not yet established a licensing regime, the new BOT P2P Notification provides P2P operators an understanding of what the future licensing laws may likely require. As it stands, this BOT P2P Notification only offers guidance to those operators seeking approval for operations falling within the regulatory "sandbox" established previously.

John Fotiadis *(Senior Member), Atherton Legal, (johnf@athertonlegal.com)*.

Tichachad Yingluecha, *(Associate Lawyer), Atherton Legal (tishay@athertonlegal.com)*

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.