Available online at www.sciencedirect.com

ScienceDirect

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

Computer Law & Security Review

Asia Pacific news

*Gabriela Kennedy**

Mayer Brown, Hong Kong

ARTICLE INFO

Article history:

Keywords:
Asia-Pacific
IT/Information technology
Communications
Internet
Media
Law

ABSTRACT

This column provides a country-by-country analysis of the latest legal developments, cases and issues relevant to the IT, media and telecommunications' industries in key jurisdictions across the Asia Pacific region. The articles appearing in this column are intended to serve as 'alerts' and are not submitted as detailed analyses of cases or legal developments.

1. Hong Kong

Gabriela Kennedy (*Partner*), *Mayer Brown* (gabriela.kennedy@mayerbrown.com);
Karen H.F. Lee (*Senior Associate*), *Mayer Brown* (karen.hf.lee@mayerbrown.com).

1.1. *Computer Says No – Prosecuting Smartphone Offences*

In the recent Hong Kong case of *Secretary for Justice v. Cheng Ka-Yee and Ors* ("**Case**"), the Court of First Instance ("**CFI**") allowed an appeal concerning the offence of obtaining access to a computer for dishonest gain under Section 161(1) of the Crimes Ordinance (Cap.200) ("**CO**"). The impact of the decision goes well beyond the circumstances of the Case, and may even act as a barrier to prosecuting individuals who take upskirt photos or engage in other questionable activities using their smartphones.

1.1.1. *Background*

The four defendants were all primary school teachers. In preparation for student admission interviews to be held at the school where three of the defendants worked, a teachers' briefing session was organised for the day before. During the briefing session, two of the defendants took photographs of the interview questions using their smartphones, and sent them to a friend as well as to the third defendant, who was late for the briefing. The third defendant later copy typed the interview questions into a Word file on the school's desktop computer before emailing the file to the second defendant and a third party. The Word file was then forwarded by the second defendant to the fourth defendant via email, who took photographs of the Word file and sent them to her friends using her smartphone.

The defendants were charged under Section 161(1)(c) of the Crimes Ordinance (Cap.200) ("**CO**") with the offence of obtaining access to a computer with a view to dishonest gain for another. The prosecution argued that the "dishonest gain" was the opportunity for parents to prepare their children for the school interviews in order to improve their chances of gaining admission to the school.

At trial, there was no dispute that the smartphones used by the defendants were, in effect, computers; in *Secretary for Justice v. Wong Ka Yip Ken*, it was held that smartphones fell within the definition of a computer for the purposes of Section 161(1)

* Corresponding author: Mayer Brown, 16th - 19th Floors, Prince's Building,10 chater Road, Hong Kong
E-mail address: gabriela.kennedy@mayerbrown.com

https://doi.org/10.1016/j.clsr.2018.10.003
0267-3649/

of the CO. The main focus of the Magistrate was whether or not the element of dishonesty was established.

The Magistrate held that there was reasonable doubt as to whether the teacher in charge of the admission process had made it clear to the defendants the confidential nature of the briefing. Further, the Magistrate noted that the photographs taken by the first and second defendants were done in the presence of other people at the briefing (including the teacher in charge of admissions). In light of the foregoing and other findings, the Magistrate held that the prosecution failed to prove the element of dishonesty for the purposes of establishing an offence under Section 161(1)(c) of the CO. As a result, the defendants were acquitted.

1.1.2. *Appeal*

On appeal, however, a new question was put to the prosecution by the CFI – whether the *actus reus* for the offence (i.e. obtaining access to a computer) could even be proved. The CFI raised the concern that a number of cases have been brought before the court for a wide range of wrongful acts under Section 161(1)(c) of the CO, simply on the basis that a smartphone has been used in the commission of the act, which (if not for the use of the smartphone) would not have been criminal. For example, the taking of upskirt photos or sending confidential information to third parties.

The CFI gave the example of two individuals meeting face-to-face to discuss a plan to commit a crime, but they later decide to abandon the idea. Such a meeting is unlikely to amount to an offence. However, if they discussed the matter through the use of a smartphone, then according to the prosecution's interpretation of Section 161(1)(c) of the CO, such an act would amount to an offence. As stated by the CFI, "if that is the legal position, then whether or not they should be punished under criminal law would depend on the devices they used to communicate... I fail to see the logic and legal basis in converting improper acts which are not otherwise offences under established legal principles into an offence under Section 161 simply because a computer was involved in the commission of such misconducts."

The CFI held that the ambit of the *actus reus* for the offence (i.e. obtaining access to a computer) under Section 161(1)(c) of the CO should be limited to the unauthorised extraction and use of information from a computer. Therefore, in this Case, since three of the defendants had used their own smartphones to take the photographs and to send or receive them, and another defendant's use of the school's computer to create the Word file was not unauthorised, their actions did not amount to an unauthorised extraction and use of information from a computer.

The appeal was dismissed.

1.1.3. *What is the impact of the Case?*

The outcome of this Case may have seemed innocuous, but has in fact dealt with a blow to the ability to prosecute many smartphone-related crimes, in particular the taking of upskirt photos. The judgment has resulted in several pending smartphone-related cases being adjourned or dropped.

Section 161 was originally drafted to prevent computer crimes such as hacking, but has been expanded to criminalise other conduct that, whilst reprehensible, may not clearly fall under other criminal offences or may be more difficult to prosecute under other legislation. For example, the taking of upskirt photos or the leaking of exam questions. Such broad application of the offence has been condemned by some as going too far and acting as a "catch-all-offence", whilst others have praised it as providing a solution to criminalise reprehensible conduct.

On 6 September 2018, the Department of Justice's application for a further appeal to be heard before the Court of Final Appeal was granted. The Department of Justice argued that the CFI's judgment was too narrow, and was not in accordance with the intention of the legislation. The CFI's interpretation could even have the potential effect of de-criminalising certain cyber attacks, e.g. the sending of an email through the sender's own computer to transmit a virus to cause disruption to the recipient's IT systems.

1.1.4. *Takeaway Points*

The Case demonstrates how current legislation may be inadequate to deal with the digital age. Many actions are widely seen as criminal because they involve the use of smartphones or computers, when in fact they do not squarely fall under an existing offence. Department of Justice and the courts have had the burden of trying to give new meaning and interpretation to old laws in order to deal with the ever-changing nature of crimes enabled by technology.

However, it may be time for a revamp of the legislation to directly address these issues. As a step towards this, on 16 May 2018, the Law Reform Commission's Review of Sexual Offences Sub-committee published a consultation paper making preliminary proposals for the reform of law concerning miscellaneous sexual offences. This is the government's chance to introduce the taking of upskirt photos as an offence, something that was recommended by the Hong Kong Bar Association in its comments on the consultation paper issued on 16 August 2018.

2. Australia

Philip Catania *(Partner), Corrs Chambers Westgarth* (philip.catania@corrs.com.au);
Arvind Dixit *(Partner), Corrs Chambers Westgarth* (arvind.dixit@corrs.com.au)

2.1. *The new Consumer Data Right – issues and opportunities*

Businesses who hold data about consumers need to be aware of a number of significant changes arising from the proposed new Australian Consumer Data Right ("**CDR**"). The proposed legislation has been released for public comment, and may be altered depending on submissions received by the Government and further Government analysis. It is clear from the Government's position, however, that a new CDR right will come into effect in Australia.

The new CDR is intended to come into effect on 1 July 2019 for participants in the banking sector, however it will soon after be implemented in the energy and telecommunications sector, with other sectors to follow. The reference to "sectors"

is a little generic – the CDR will more so apply to particular classes of entities and particular datasets that will be designated by the Federal Government.

At its core, the CDR allows a consumer to obtain certain data held about that consumer by a third party and to enable that data to be given to certain accredited third parties for certain purposes (including to enable comparisons between services to be made).

2.1.1. *Issues and Opportunities*

While the mantra of the new CDR is all about consumer choice and competition, there are some potentially significant imposts which could have substantial compliance cost impacts on the data providers and could impact on data innovation.

At the same time however, there are opportunities for organisations to provide services and products that support and enhance consumer choice through the innovative use of valuable datasets that were previously difficult to obtain.

Below are some of the significant issues and opportunities that may arise for organisations as a result of the proposed CDR:

(a) **Business information** – the CDR applies to any type of consumer who is seeking information. It is not limited to individuals. In the words of the explanatory materials to the CDR *"the CDR consumer is a person, including a small, medium or large business enterprise…"*. Potentially, large business organisations can obtain data about the use of a particular service from a service provider and transfer that information to a competitive service provider. While there are "privacy safeguards" in place, it is unclear how confidential and sensitive information will be dealt with.

(b) **Not limited to personal information** – as is evident by the fact that businesses can obtain information about their use of a particular service, individuals can obtain data about their use of the service and that data does not need to be "personal information" as defined in the Privacy Act. In other words, the data does not have to be information from which the identity of the individual can be identified. All it needs to be is information that "relates to" the consumer. This potentially broadens the field of data that must be made available to the consumer. The extent of that requirement will need to be set out in the yet to be promulgated "Consumer Data Rules". The Australian Competition and Consumer Commission ("ACCC") is planning on releasing the Consumer Data Rules for the banking sector in the week of 10 September 2018.

(c) **Privacy safeguards** – while they are very similar to aspects of the Australian Privacy Principles, there are a new set of principles called the Privacy Safeguards that need to be adhered to when it comes to CDR data. Organisations will need to be set up so that they can properly deal with the requirements of the Privacy Safeguards in the same way that they have been geared up to deal with the Australian Privacy Principles. This may necessitate keeping CDR data segregated from other business data so that the specific requirements of the Privacy Safeguards can be complied with. If an organisation is also subject to the EU General Data Protection Regulation ("GDPR"), this could potentially mean having three sets of segregated data which cannot be mixed.

(d) **Technical requirements** – because consumers will be able to request that their consumer data be transferred from a data holder to an accredited organisation under the CDR, the data holders need to have their systems set up to be able to deal with this transfer of data. This raises two issues for data holders:

  (i) the nature of the systems that have been established to allow this transfer to occur and what changes need to be made to them; and

  (ii) the format and nature of the data that is required to be transferred.

The latter is to be specified initially by Data 61 which is the inaugural Data Standards body.

(a) **Contractual obligations** – as we've seen with the Australian Privacy Principles and most recently with the GDPR, we can expect to see organisations placing contractual obligations on their service providers to give effect to those organisation's obligations under the CDR. Get ready for another round of contractual amendments.

(b) **Value added information** – CDR data that needs to be shared includes information that is "directly or indirectly derived" from the CDR data. Where a company has augmented customer data with its own information to create unique insights in relation to a consumer, this would potentially need to be shared. This may be seen by some to potentially impact on innovative data applications.

(c) **Third Party datasets** – CDR data could potentially include third party data sets, which the data holder may not have rights to share. It is contemplated that there may be compensation where an organisation is compelled to disclose proprietary data as part of the CDR arrangements, but the process of valuing this data is yet to be outlined.

(d) **Reciprocity** – the concept of "reciprocity" refers to the fact that if an organisation wants to be the recipient of CDR data (that is, if it becomes "accredited"), it should also be required to share data that it holds to other recipients. It is not entirely clear how this concept will operate where the recipient does not hold data, which falls within one of the relevant datasets that has been designated for a sector, e.g. a comparison service.

(e) **Consent** – the precise details of what will be required for a consumer to "consent" to disclosure are still to be worked out and will be set out in the Consumer Data Rules. It may be that the consent requirements for CDR Data will be different from consent and related notice requirements under the Privacy legislation.

(f) **Accreditation** – the ACCC is finalising its position paper on the requirements that organisations must meet in order to become accredited to receive CDR data. In addition to the principle of "reciprocity" referred to above, another important point to note on "accreditation" is that those organisations who may have been exempted from complying with Australia's Privacy Principles in relation to "personal information" (e.g. small business operators) will lose that exemption if they become accredited under the CDR scheme.

We will provide further updates as the Government issues the Consumer Data Rules and responds to submissions and industry reaction.

The above is only a general outline of some of the key features of the proposed CDR regime. It should not be taken as an expression of the definitive position given the draft nature of the proposed legislation and the fact that comment is still being sought, and it should not be taken as legal advice.

3. Japan

Kiyoko Nakaoka *(Attorney-at-Law, Patent Attorney), Kubota* (nakaoka@kubota-law.com)

3.1. *Protection of Big Data under Unfair Competition Prevention Act*

3.1.1. *Introduction*

The National Diet of Japan approved a bill for the partial revision of the Unfair Competition Prevention Act ("Revised Act"), which was aimed at enhancing data protection, on 23 May 2018. The Revised Act will come into effect on 1 July 2019.

With the growth of the Internet of Things and artificial intelligence, the Revised Act is expected to further facilitate the use of data including big data. In order to actively distribute data to the market and encourage appropriate utilization of data, it is necessary to develop a business environment that can utilize data safely and securely.

Under the current laws, it has been difficult to protect valuable data sets, such as big data, because such is not protected under either the Patent Act or the Copyright Act. Moreover, any data that is meant to be shared cannot fall into the category of a "trade secret", which is protected under the Unfair Competition Prevention Act. However, data is easy to duplicate and distribute, and once it has been illegally distributed, damages may expand rapidly and widely.

In view of such circumstances, the Revised Act introduces the new element of an "act of unfair competition" in relation to the protection of data. Under the Revised Act, wrongful acquisition and use of valuable data is deemed to be an "act of unfair competition". Victims will be able to seek an injunction against such an act of unfair competition and enjoy favourable treatment in the calculation of damages.

The Revised Act also aims to target a range of other "acts of unfair competition" relating to technological restriction measures, including providing services or devices that circumvent such measures for users. This article will focus on the protection of valuable data only.

3.1.2. *Protection of Valuable Data*

(a) Valuable Data protected by the Revised Act

Under the Revised Act, the concept of "limited offer data" ("**Limited Offer Data**") is introduced as a type of valuable data to be protected. For data to be deemed as Limited Offer Data it must meet the following criteria:

(i) the data should only be provided to a limited number of users;
(ii) a considerable amount of the data must be stored by an electromagnetic method and managed; and
(iii) the data shall be related to technical or business information.

However, since a "trade secret" is already protected under the current Unfair Competition Prevention Act, trade secrets are excluded from the protection provided to Limited Offer Data.

For example, three-dimensional map data provided for automatic travelling vehicles, sales data for each product collected by the point of sale system, and the Revised Act will protect data summarizing technical information on chemical materials.

(b) Acts of Unfair Competition Prohibited under the Revised Act

Under the Revised Act, the following four categories of acts are prohibited:

(i) acquiring the Limited Offer Data by means of theft, fraud or other illegal means, or using or disclosing the Limited Offer Data acquired by such means;
(ii) acquiring the Limited Offer Data while knowing that the Limited Offer Data was illegally acquired in the first place, or using or disclosing such acquired Limited Offer Data;
(iii) in the case where the Limited Offer Data is duly acquired from its owner, using or disclosing the Limited Offer Data for the purpose of obtaining fraudulent profits or damaging the owner in a manner that is e equivalent to misappropriation or breach of trust; and
(iv) in the case where the Limited Offer Data is acquired without knowledge that it was illegally acquired or disclosed, disclosing the Limited Offer Data beyond the scope of the contract between the provider and the acquirer after discovering that the Limited Offer Data was illegally acquired or disclosed.

For example, the following acts will be prohibited by the Revised Act:

(i) an act of hacking a server of a data provider by using an ID and a password of an authorised person without permission and copying that person's private data to another computer;
(ii) an act of receiving the data from a hacker while knowing that the data was acquired in an unauthorised manner;
(iii) in the case where a data receiver is requested to analyze data exclusively for the data provider and is prohibited from using the data for other purposes, and the data receiver uses the data for another purpose without first obtaining the data provider's permission and develops software for another company for illegal profit; and
(iv) although a data distributor has knowledge that the data provider illegally acquired the data after purchasing it, he continues to resell the data to other companies. However, if the data distributor concluded a contract for

reselling the data for "X" years with the data provider before knowing that it was illegally required, reselling the data during "X" years does not fall into "an act of unfair competition".

(c) Remedies

Victims suffering damage caused by the above acts of unfair competition in relation to the Limited Offer Data may be entitled to civil remedies under the Revised Act, such as an injunction, damages and so on.

(d) Guidelines

In order to clarify the contents of the revised provisions, guidelines will be established to provide specific examples of actions that do or do not fall into acts of unfair competition before the enforcement date of the Revised Act.

4. Macau

Julia Herold *(Partner), DSL Lawyers* (jherold@dsl-lawyers.com)

4.1. *Telecommunications and Cybersecurity Regulation in Macau – What Lies Ahead?*

4.1.1. *Overview*

Macau has a sophisticated, independently regulated communications market due to the city's status as a Special Administrative Region ("**SAR**") of the People's Republic of China ("**PRC**") following the handover from Portugal. Gradual liberalisation of the market has opened up the telecoms industry and the millions of visitors that visit the tiny enclave every year significantly drive demand for telecom services.

Until 1999, the year of the handover to the PRC, the incumbent operator, Companhia de Telecomunicações de Macau SARL ("**CTM**") held exclusivity on fixed, mobile and internet services and networks. After enacting new laws to liberalise the market in 2001, the regulatory activity has stalled somewhat.

Fixed networks and related services were liberalised in 2011, with a new licence granted to Companhia de Telecomunicações MTel ("**MTel**") in 2013.

Since then, there have been no changes in the telecommunications legal and regulatory framework.

Currently, the structure of the telecommunications regulation is still vertical. There are separate sets of regulations and licences on fixed, mobile and internet services and respective networks, as well as separate regulations on broadcasting, cable TV and satellite TV services.

CTM and MTel hold a licence for fixed services and networks. There are four licensed mobile operators: CTM, 3 Macau (Hutchison), SmarTone Macau and China Telecom Macau. Regarding Internet services, there are 23 Internet Service Providers ("**ISP**") who are operating in Macau, including all the above five operators.

Macau's mobile market competition is intense, with mobile penetration in excess of 200% due to multiple SIM card ownership as well as sales of SIM cards to visitors.

CTM still maintains the exclusive right to operate all fixed network infrastructure and related services owned by the Macau SAR government under the CTM Concession. This right is given as a type of management lease contract whereby the Macau government appoints CTM to operate and maintain the concession assets owned by the Macau SAR government, such as ducts, cables, etc.

Macau Cable TV has been given a further 25-year concession to operate terrestrial subscription TV services on a non-exclusive basis in 2014, and there are a small number licensed operators to provide satellite TV broadcasting services.

4.1.2. *Transition to Convergence*

In its policy addresses of the last few years, the Macau government has been announcing their intention to introduce the licensing of triple play networks. In the address for 2018, it stated that the task of preparing a proposed law on triple play licensing was not concluded in 2017, due to the need to expand and improve the initial project after a new analysis of the current status of telecommunications market. The government announced that it is presently working on the "Network and Services Convergence Regime".

It is not clear when the draft laws will be finalised, but in recent statements, the Secretary for Transport and Public Works – who oversees the telecommunications sector – said that the new proposed convergence laws may "take years" to be completed, as they require repealing the existing ones and creating a whole new legal and regulatory framework.

It is indisputable that a transition from the outdated current laws to a full convergence regime is a challenging task. Apart from the profound update of the legal and regulatory framework, the transitional arrangements and integration of existing concessions / licenses and the safeguard of the holders' rights and interests are also issues that need to be considered. Another challenge is to keep up with the constantly evolving technologies. Given the rapid pace of change in technology, compared with the time needed to introduce and implement new legislation, the new framework needs to be broad enough to adapt to the introduction of new products and services.

In spite of the challenges, there is an urgent need to implement revised and more convergent or horizontal regulation – to wait a few more years would be a detriment to the telecommunications market and ultimately harmful to the consumers and operators. One example where Macau is losing out is wireless Internet of Things and the installation and operation of low-power wide-area networks or LPWANs, for which there is demand but no licensing or regulation in place.

However, it is not an impossible task, provided that the government is willing to hire a team of experts from the neighbouring jurisdictions whose regulatory frameworks are more advanced, such as Hong Kong and Singapore. The government should also take advice from Portugal, where the Electronic Communications Law – adapted from the Directives of the European Commission (s 2002/19/CE, 2002/20/CE, 2002/21/CE, 2002/22/CE and 2002/77/CE) – is in force since 2004 (with various amendments introduced over the years) and where the legal system is very similar to that of Macau. There is certainly enough money to obtain the best possible expertise. Macau's

fiscal surplus grew 86.2% in 2017, amounting MOP 40.38 billion (approx. USD 5 billion).

4.1.3. *The Cybersecurity Law*

Between December 2017 and January 2018, the Macau government published a consultation paper on the proposed Cybersecurity Law for comments to the industry, the legal community and ordinary citizens.

The proposed draft law has not been made available to the public yet.

In summary, the features of the new law as they are known from the consultation paper are as follows:

(a) Telecommunications operators and ISPs would be responsible for implementing a "real name" registration system, including prepaid SIM cards;
(b) The law mandates that ISPs retain their users' online activity logs for at least one year;
(c) It provides for the establishment of a cybersecurity standing committee and a cybersecurity incident alert system, as well as an emergency centre intended to deal with any cybersecurity threats. The committee will be authorized to monitor online data traffic in binary code, as well as to keep track of and investigate future cyberattacks;
(d) Companies from the private sector operating in 11 crucial sectors would enforce protection measures, including internet operators and mass media, water and energy supply, financial systems, gaming, and health, among others;
(e) These sectors would be under the supervision of related government departments and authorities (e.g. the Macau Monetary Authority upon receiving instruction from the cybersecurity emergency centre would be responsible for overseeing the implementation of measures in the banking and financial systems);
(f) Officers from the cybersecurity emergency centre will be guaranteed the right to enter the offices and facilities of internet operators (in both the private and public sector) for inspection and operators are required to cooperate and provide any information that is requested by them;
(g) Operators will be required to fulfil all reasonable requests of the officers and to follow any instructions they issue on the maintenance of their communication networks; and
(h) Penalties for non-compliance with the law may be as high as MOP 500 million (approximately USD 62 million).

In spite of the government officials' assurance that authorities would not monitor individual online activities or restrict freedom of speech, local associations have expressed serious concerns.

In the consultation document, there is no mention of a court order in respect of the officers' rights to enter the internet operators' offices for inspection and request of any information. "Inspection" and "any information" are very broad concepts and can open the door to monitoring of online activities and indirect exercise of censorship. At the minimum, the law should require a Court order if the inspection includes obtaining information on individuals' private communications and online activities.

Another concern that has been heard during the consultation period is the extent of powers granted to the cybersecurity standing committee, in particular the monitoring of online data traffic in binary code, which some consider to allow online monitoring and to be insufficient to safeguard people's fundamental rights to privacy and freedom of speech under the Basic Law.

Until the Legislative Assembly approves the final draft law, there will certainly be much debate and criticism. However, we do not expect the main features of this law to undergo fundamental changes.

5. Malaysia

Charmayne Ong *(Partner), Skrine* (co@skrine.com)

5.1. *Role of E-Wallets in Malaysia's Cashless Future*

5.1.1. *Introduction*

In line with the global trend, Malaysia in her bid to transform herself into a cashless society has seen an unprecedented increase over the recent years in electronic wallet ("**e-wallet**") operators offering a host of electronic money ("**e-money**") products. Local and international players have both entered the scene to tap into the Malaysian e-wallet market. Several factors point towards Malaysia being a nation well placed to embrace the e-wallet trend. For instance, according to the Department of Statistics Malaysia ("**DOSM**"), Internet penetration of the Malaysian market stood at 85.7% in 2017. Further, according to the Malaysian Communications and Multimedia Commission ("**MCMC**"), smartphone penetration of the Malaysian population has risen to 75.9% in 2017. The MCMC also reports that smartphones remained the most popular means for Malaysians to access the Internet in 2017, making Malaysia a mobile-oriented society.

As such, with the prevalence of smartphones and accessibility of the Internet, Malaysia appeared to be ripe for entry of e-wallets. Indeed, according to the latest statistics published by the Central Bank of Malaysia or Bank Negara Malaysia ("**BNM**"), the number of network-based users of e-money for the first half of 2018 alone saw an increase of nearly 30% when compared to the entire year of 2017, and nearly 165 times when compared to the entire year of 2005. As part of BNM's drive for a cashless society, BNM has also shifted its focus in 2018 on promoting mobile payments, which will greatly affect the adoption of e-money in Malaysia.

5.1.2. *What is E-Money?*

BNM defines e-money as "*a payment instrument that contains monetary value that is paid in advance by the user to the e-money issuer.*" According to BNM, e-money can be issued in different forms, such as card based (e.g. prepaid card) and network-based which can be accessed via the Internet, mobile phones or any other devices.

5.1.3. *How is E-Money Governed?*

Before the Financial Services Act 2013 ("**FSA**") was enacted, e-money was governed under the Payment Systems Act 2003 (repealed by the FSA). E-money is now governed under the FSA as a payment instrument. Under the FSA, issuers of designated payment instrument ("**DPI**") are required to obtain

BNM's prior approval. Empowered by the FSA, BNM has prescribed e-money as a DPI under the Financial Services (Designated Payment Instruments) Order 2013 ("**DPI Order**"). Order 2 of the DPI Order includes "*electronic money that is any payment instrument, whether tangible or intangible, that- (i) stores funds electronically in exchange of funds paid to the issuer; and (ii) is able to be used as a means of making payment to any person other than the issuer.*"

BNM has also prescribed several requirements under the E-money Guidelines with various operational requirements in the form of principles such as the requirement to establish adequate governance and operational arrangements, to ensure proper risk management is in place, to ensure prudent management of funds etc. E-money issuers are prohibited from, among others, issuing e-money at a discount, extending loans to other persons using the money collected, extending credit to the users etc. It is also worth noting that e-money issuers are required to be locally incorporated and must ensure that all transactions in Malaysia are in Malaysian Ringgit. They are also required to comply with, among others, the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001.

5.1.4. *What is happening in 2018?*

On 20 March 2018, BNM issued the Interoperable Credit Transfer Framework ("**ICTF**") after taking into account the public feedback received. The operationalisation of the ICTF was stated to be an area of primary focus by BNM in 2018 in BNM's 2017 Report. The ICTF has since come into effect on 1 July 2018.

The ICTF is essentially the establishment of a shared payment infrastructure to enable interoperability of credit transfer services, which would expand network reach and avoid market fragmentation. This would affect both inter-bank credit transfers and inter-scheme (e-money) credit transfers. All such credit transfers must be processed in Malaysia through the operator of the shared payment infrastructure, Payments Network Malaysia Sdn. Bhd. ("**PayNet**"), an entity partly owned by BNM. This increases BNM's regulatory oversight on the credit transfer system to ensure the safety and integrity of the same.

A crucial part of the ICTF is the establishment of the Real-time Retail Payments Platform ("**RPP**") by PayNet which consists of: (i) the National Addressing Database ("**NAD**") which links a bank or e-money account to common identifiers ("**CI**") of an account holder (e.g. mobile phone number, identification number, company/business registration number) which would be used to facilitate payment; and (ii) an interoperable Quick Reference ("**QR**") scheme and common QR codes which allow customers to make and receive payments. According to PayNet's Technology Roadmap, the RPP remains at its infancy stage as it is currently undergoing testing and on-boarding of banks between December 2017 and October 2018.

Under the ICTF, "eligible" issuers of e-money must, among others, ensure that its customers are able to make payment to and receive payment from another customer of the same or another "eligible" issuer of e-money either through use of the RPP i.e. customers of e-wallet X must be able pay and receive e-money from customers of e-wallet Y. Transaction fees for eligible credit transfer transactions under RM5,000 must also be waived. These requirements, however, appear to only apply to issuers of e-money which are eligible according to the ICTF (e.g. issuers with 500,000 active users for 6 months consecutively).

5.1.5. *Road Ahead*

With the sudden increase in e-wallets in Malaysia, it begs the question of whether e-wallets and e-money would take over electronic payment in Malaysia and become the future of Malaysia's cashless society in the making. Whilst BNM has been very supportive in encouraging growth in this area, e-wallets nevertheless face a number of challenges in Malaysia.

One of the biggest obstacles in the widespread adoption of e-wallets, apart from cybersecurity risks, is the availability and sheer convenience of payment cards such as debit cards over e-wallets. Indeed, BNM does not anticipate that mobile payment would replace debit cards and credit transfers in displacement of cash and cheques, but expects the former to *complement* the latter to accelerate the displacement of cash and cheques. However, with the waiver of transactions fees for credit transfers under RM5,000 and the cost effectiveness of not requiring a Point-of-Sale Terminal, the future of e-wallets in Malaysia remains promising.

This article was first published/released in Euromoney's Women in Business Law Expert Guide 2018.

6. Singapore

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

Quek Zhao Feng *(Associate), WongPartnership LLP* (zhaofeng.quek@wongpartnership.com)

6.1. *Cybersecurity Act 2018 And Subsidiary Legislation Come Into Force*

As of 31 August 2018, key provisions of the Cybersecurity Act (Act 9 of 2018) (the "**Act**") and relevant subsidiary legislation (i.e. the Cybersecurity (Critical Information Infrastructure Regulations 2018) ("**CII Regulations**") and Cybersecurity (Confidential Treatment of Information) Regulations ("**CTI Regulations**")) have come into force.

The Act and subsidiary legislation establish a general legal framework for the oversight and maintenance of national cybersecurity in Singapore through inter alia:

(a) establishing a framework for the designation of essential computers and computer systems as Critical Information Infrastructure ("**CII**");
(b) authorising new investigative powers for the Singapore Cyber Security Agency ("**CSA**") to prevent and respond to cybersecurity threats and incidents; and
(c) establishing a framework for the sharing of cybersecurity information between computer systems to assist with the identification of shared vulnerabilities within said systems and the prevention of cybersecurity incidents.

Other provisions of the Act not yet in force mainly concern a licensing framework for cybersecurity service providers providing: (i) penetration testing; and (ii) managed security

operations centre monitoring services. These provisions are slated to come into force only in the second half of 2019.

6.1.1. The CII Framework

Under the Act, the Commissioner of Cybersecurity ("**Commissioner**") has the discretion to designate a computer or computer system as a CII if the Commissioner is satisfied that:

(a) the computer or computer system is necessary for the continuous delivery of an "essential service", with the loss or compromise of said computer or computer system having a "debilitating effect" on the availability of said essential service in Singapore; and
(b) the computer or computer system is wholly or partly located in Singapore.

Where the Commissioner reasonably believes that a specific computer or computer system may fulfil the above CII criteria, he or she may also require persons exercising apparent control over the CII to furnish information for the purposes of ascertaining whether said computer or computer system is a CII.

The Act imposes enhanced statutory obligations on CII designees proactively to safeguard their systems against cyber-attacks. Owners of a CII are obliged to:

(a) undergo cybersecurity exercises for readiness testing purposes;
(b) abide by official CII Codes of Practice or written directions that the Commissioner may issue or approve;
(c) inform the Commissioner of any change in the beneficial or legal ownership in a CII within 7 days from the date of such change;
(d) undergo regular bi-yearly audits of its CII for compliance with the Act, any codes of practice and standards of performance, and furnish a report of the same; and
(e) undergo yearly cybersecurity risk assessments;

With reference to the list above, failure to comply with obligation (a) constitutes an offence rendering a CII owner liable to monetary penalties. Failure to comply with obligations (b) and (c), and written or statutory directions prescribed for audits and cybersecurity risk assessments under obligations (d) and (e), is a statutory offence, rendering the CII owner liable to monetary penalties, a custodial sentence, or both.

Finally, the Act and CII Regulations also provide a framework for CII owners aggrieved by the Commissioner's decisions or directions (including the decision to designate a computer or computer system as a CII) to appeal said decision or directions to the Minister. The CII Regulations themselves provide clarity on several practical aspects of the Act's CII-related provisions, including:

(a) the relevant types of information that must be furnished by CII owners or potential CII owners pursuant to the Commissioner's request;
(b) in the event of occurrence of a cybersecurity risk assessment, the types of information to be submitted and relevant time frame for said submission;
(c) the manner and form of a cybersecurity risk assessment (as defined under the Act) and mandatory objectives it must fulfil; and
(d) the manner and form for submission of appeals by CII owners to the Minister.

6.1.2. Investigative Powers of the CSA

The Commissioner has also been granted additional investigative powers under the Act to:

(a) require any person to answer questions or provide written statements,
(b) produce records or information and inspect, copy or take extracts from any person; and
(c) orally examine any person appearing to be acquainted with the cybersecurity threat or incident,

for the purposes of assessing the impact or potential impact of a cybersecurity threat or incident, or the prevention of any harm or further harm from that incident or any subsequent cybersecurity threat or incident arising from the same.

Where the Commissioner is of the opinion that the cybersecurity threat or incident is severe enough to create: (i) a risk of significant harm being caused to a CII; (ii) a risk of disruption to the provision of an essential service; or (iii) a threat to national security or key public sectors, or the incident is in general disruptive enough having regard to the persons, computers or computer systems and the information put at risk, the Commissioner is authorized under the Act to exercise additional powers. These include the power to:

(a) access the premises of the computer or computer systems reasonably suspected to be affected by said cybersecurity incident,
(b) access, inspect, and scan said computer or computer system for the detection of cybersecurity vulnerabilities;
(c) extract and take possession of any electronic records and computer programmes contained in a computer suspected to be affected by the cybersecurity incident; and
(d) take possession of the computer and all suspected equipment for further examination or analysis.

Lastly, the Act provides emergency powers for the Minister to prevent, detect, or counter "any serious and imminent threat to the provision of any essential service; or the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore." These emergency powers are non-exhaustive, and include the power to:

(a) authorize or direct any person to take measures or comply with requirements necessary to prevent, detect, or counter any threat to a computer or computer system or any class of computers or computer systems; and
(b) authorize the police and other authorized persons to access and inspect relevant computer operations, data, and information concerning decryption capabilities.

6.1.3. Information Sharing Framework and the CTI Regulations

Though the Act does not oblige owners of computers and computer systems to take proactive steps in sharing system

information, the Act facilitates the sharing of such information by imposing obligations on CII owners to furnish CII-related information on the Commissioner's request. Such information includes information on the:

(a) design, configuration and security, and operations of the CII or any other computer or computer system interconnected with that CII; and
(b) such other information as the Commissioner may require to ascertain the level of cybersecurity of the CII.

The CSA actively shares useful information gleaned from these requests with the CII sectors for their appropriate preemptive or remedial action. Such information includes technical and operational information on cybersecurity threats and vulnerabilities within the CII sectors, as well as technical indicators, cyber threat signatures, and contextual cyber threat assessments.

Given the potentially sensitive and confidential nature of information provided pursuant to such requests, the Act also contains provisions that:

(a) create an obligation on "specified persons" to preserve the secrecy of all matters relating to the: (i) computer or computer system; (ii) business, commercial or official affairs; (iii) confidential subject matter; and (iv) identity of the information furnisher; and
(b) establish a procedural framework through which the information furnisher may claim such information as confidential (i.e. to claim entitlement of the same information to the aforementioned secrecy obligations in (a)).

The procedural framework in (b) is clarified by the CTI Regulations, which *inter alia*, prescribes the steps the information furnisher must take to make the relevant claim.

6.1.4. *Comments*

The Cybersecurity Act establishes a framework for designating critical infrastructure systems in essential sectors and imposing obligations on the owners of these systems to proactively address cybersecurity concerns – it therefore addresses cybersecurity concerns more proactively, instead of the more traditional approach of criminalizing cyberattacks (which in Singapore is addressed by other existing laws).

6.2. *PDPC Issues Advisory Guidelines on Personal Data Protection Act for NRIC And Other National Identification Numbers*

The Personal Data Protection Commission ("**PDPC**") has on 31 August 2018 issued its Advisory Guidelines on the Personal Data Protection Act (No.26 of 2012) ("**PDPA**") for NRIC and other National Identification Numbers (the "**Guidelines**").

The Guidelines clarify how the PDPA applies to an organisation's: (i) collection, use, and disclosure of NRIC numbers (or copies of NRIC) and other national identification numbers (i.e. Birth Certificate numbers, Foreign Identification Numbers ("**FIN**") and Work Permit numbers); and (ii) the retention of physical NRIC's. The PDPC intends to apply the interpretation of the PDPA in line with these Guidelines from **1 September 2019** onwards.

By way of background:

(a) The PDPA establishes a general data protection law in Singapore which applies to govern the collection, use and disclosure of personal data by organisations. In brief, organisations are subject to a number of data protection obligations under the PDPA, including:
    (i) having reasonable purposes, notifying purposes, and obtaining consent for the collection, use or disclosure of personal data;
    (ii) allowing individuals to access, and correct their personal data;
    (iii) taking care of personal data (including the accuracy thereof), protecting personal data (including in the case of international transfers), and ceasing to retain personal data if no longer needed; and
    (iv) having policies and practices to comply with the PDPA.
(b) The PDPC (tasked among its functions with administering and enforcing the PDPA), launched on 7 November 2017 a public consultation seeking the general public's views and comments on: (i) the collection, use and disclosure of NRIC numbers; and (ii) retention of physical NRICs by organizations ("**Public Consultation**").
(c) Following the responses received pursuant to the Public Consultation, the PDPC has consolidated and addressed them in the Guidelines.

6.2.1. *Collection, Use or Disclosure of NRIC numbers (or copies of NRIC)*

The PDPC has clarified in the Guidelines that organisations are generally not allowed to collect, use, or disclose NRIC numbers (or copies of NRIC), unless the following exceptions apply:

(a) Collection, use or disclosure of NRIC numbers (or copies of NRIC) is required under the law (or an exception applies under the PDPA) ("**Exception A**"); or
(b) Collection, use or disclosure of NRIC numbers (or copies of NRIC) is necessary to accurately establish or verify the identities of the individuals to a high degree of fidelity ("**Exception B**").

For Exception A, the following situations are listed as examples of where collection, use or disclosure of NRIC numbers (or copies of NRIC) are required for legal compliance purposes:

(a) Healthcare organisations (e.g. hospitals and clinics) may obtain their patients' NRIC information for identity verification purposes (they are statutorily required to maintain accurate, complete and up-to-date medical records of their patients);
(b) Hotels are statutorily obliged to require the full names and NRIC numbers from every hotel guest seeking accommodation;
(c) Telecommunications service providers are statutorily required to collect their customers' NRIC information and a copy of their NRIC when providing them with mobile phone services;

(d) Licensees of massage establishments are statutorily obliged to require prospective customers to furnish their identity card number or passport particulars;
(e) Private education institutions are statutorily obliged to keep proper records of enrolled students' NRIC numbers; and
(f) Employers are statutorily obliged to maintain detailed employment records of their employees (including employees' NRIC numbers and other relevant information).

In addition, in circumstances where the collection, use or disclosure of the individuals' NRIC number (or copy of the NRIC) is necessary to respond to an emergency threatening the data subject's health, this would qualify as a PDPA exception under the Guidelines (permitting collection, use or disclosure of the NRIC number (or copy of the NRIC)).

For Exception B, the PDPC considers it necessary to accurately establish or verify said individual(s) identity to a high degree of fidelity in situations where the inability to do so either:

(a) poses a significant safety or security risk (e.g. screening preschool visitors where children's safety is an overriding concern); or
(b) poses a risk of significant impact or harm to an individual and/or the organisation (e.g. fraudulent claims pertaining to healthcare, financial or real estate matters).

The PDPC clarified that organisations should always assess whether their specific situations fulfils the above considerations in Exception B before collecting the individuals' NRIC number (or copy of the NRIC), and the same organisation should be able to provide justification for its decision to do so upon the individual's and/or PDPC's request.

6.2.2. *Retention of Physical NRIC and Alternatives to NRIC Collection*

The PDPC also provides that organisations should generally not retain an individual's physical NRIC unless said retention is required under the law, given: (i) its importance as a unique identifier; and (ii) the potential negative impact to said individual should its security be compromised.

Accordingly, the PDPC has by way of the Guidelines, suggested that organisations adopt alternative identifiers in place of NRIC numbers, the specific identifiers to be chosen based on each organisation's own business and operational needs. Such identifiers may include:

(a) Partial NRIC numbers (e.g. the last three numerical digits and checksum of the NRIC number);
(b) Full names, vehicle numbers, and mobile phone numbers (e.g. in situations where a mall or retail outlet intends to keep records of the identities of shoppers eligible for promotions or free parking redemption); and
(c) Booking reference numbers or short-message confirmations (e.g. in situations where a cinema is required to verify identities of online movie-ticket purchasers).

The Guidelines also identify the following situations where the collection of NRIC or other identifiers may not be required:

(a) bicycle rental companies are not required under any law to collect customers' NRICs, and they should not do so as a means to ensure customers return the bicycles – a monetary deposit can be collected instead; and
(b) cigarette retailers may require checking the customer's NRIC for the purposes of verifying that the customer meets the minimum age for cigarette purchase, though the retailer should not retain a copy of the NRIC.

6.2.3. *Technical Guide to the Advisory Guidelines and Template Notice for Collection of NRIC numbers*

As an accompaniment to the Guidelines, the PDPC has also published the Technical Guide to the Advisory Guidelines on the PDPA for NRIC and other National Identification Numbers (the "**Technical Guide**"). The Technical Guide provides organisations with tips for the implementation of alternative identifiers in *new systems*, and replacement of NRICs and other national identification numbers with other identifiers in *existing systems*.

The Technical Guide also identifies the key considerations in choosing a replacement identifier for NRIC numbers as those: (i) easily remembered by the individual; (ii) unique to each individual; (iii) exempt of sensitive information; and (iv) not easily guessed by others, as well as the relevant steps and precautions an organisation should take before, during and after implementing the replacement identifier.

Where the collection of NRIC numbers is necessary or statutorily required of an organisation, the PDPC has also provided a template notice for organisations' general use. The language therein may be adapted by said organisation to obtain individuals' consent for use of their NRIC numbers.

6.2.4. *Comments*

Under the PDPA, organisations are already under the general obligation to make reasonable security arrangements to protect personal data in its possession or under its control. In a past decision by the PDPC, the Commissioner singled out the NRIC number as an example of "personal data of a more sensitive nature" which required organisations to "take extra precautions and ensure higher standards of protection under the PDPA" to comply with its obligations under the PDPA.

Given the importance of safeguarding individuals' NRIC numbers, and the potential ramifications for any abuse of the same, the Guidelines and Technical Guide provide much needed clarity for individuals seeking protection for their personal data and clear benchmarks for organisations handling NRICs.

7. South Korea

Kwang Bae Park, (Partner), Lee & Ko (kwangbae.park@leeko.com); **Hwan Kyoung Ko**, (Partner), Lee & Ko (hwankyoung.ko@leeko.com); **Sunghee Chae**, (Partner), Lee & Ko (sunghee.chae@leeko.com).

7.1. *Key Changes to the Extraterritorial Applicability of the Network Act and Cross-border Transfer Rules of Personal Information in Korea*

On 30 August 2018, the National Assembly of Korea passed a bill amending the Act on Promotion of Information and Communications Network Utilization and Information Protection ("**Network Act**") which may affect how foreign companies based abroad provide services online to users residing in Korea. This amended version of the Network Act ("**Amended Act**") was promulgated on 19 September 2018, and will take effect from 19 March 2019. The Amended Act contains several key changes regarding the extraterritorial applicability of the Network Act to foreign entities, and the cross-border transfer of personal information, among others. Key provisions of the Amended Act are summarized below.

7.1.1. *Foreign Service Providers Required to Designate a Korean Representative (Amended Act, Article 32-5)*

This new requirement is similar to Article 27 of the EU General Data Protection Regulation (which went into effect on 25 May 2018), which states that a controller or processor not established in the EU must designate a representative within the EU.

(a) Key features of Article 32-5

(i) Who will be subject to this new requirement?: (1) An information and communications service provider ("**ICSP**") or (2) an entity that receives personal information from an ICSP that (i) does not have a local address or place of business in Korea and (ii) meets the criteria established by Presidential Decree (collectively, "**Foreign Service Providers**").

(ii) Obligations of Foreign Service Providers: Foreign Service Providers must designate a corporation or individual that has an address or place of business in Korea as its representative with respect to the following tasks: (i) taking care of matters typically handled by a privacy officer (e.g. processing of user complaints), (ii) notifying/reporting data breaches to users and/or the pertinent authorities, and in cases where such notice/reporting is delayed, explaining the reason for such delay, and (iii) submitting materials to the Korean regulators responsible for enforcing the Network Act (i.e., Ministry of Science and ICT, Korea Communications Commission ("**KCC**")) that are necessary for the regulators to conduct their investigations. The Foreign Service Provider must include information regarding its Korean representative (e.g. name, contact information) in the Foreign Service Provider's privacy policy.

(iii) What happens in case of a violation?: If a Foreign Service Provider fails to designate a Korean representative in accordance with Article 35-2 of the Amended Act, the Foreign Service Provider will be subject to an administrative fine of up to KRW 20 million (approx. USD 18,000).

(b) Implications of Article 35-2

By adopting this Korean representative requirement, Korean legislators are said to be providing more explicit guidance on the extraterritorial applicability of the Network Act to foreign entities. The current version of the Network Act is silent on whether the Network Act applies to a foreign company without a local presence in Korea. However, in practice, the KCC has often taken the position that the Network Act applies to Foreign Service Providers as well. With the adoption of Article 35-2, it has become clear that Foreign Service Providers may also be subject to the Network Act. Also, given the types of tasks that the Korean representative of a Foreign Service Provider is required to perform, Article 35-2 of the Amended Act will likely be used by regulators to strengthen the enforcement of the Network Act against Foreign Service Providers. Corresponding amendments to the Presidential Decree of the Network Act have yet to be promulgated and so it may be some time before the criteria of the Foreign Service Providers who will be subject to Article 35-2 of the Amended Act become apparent. Consequently, foreign companies who provide information and communications services to Korean users are advised to continue monitoring any legislative developments on this front. Foreign Service Providers who are required to designate a representative in Korea will need to review their internal policies and practice to see whether they comply with the Network Act, and implement measures to address any identified gaps. In summary, Foreign Service Providers should take the necessary measures in advance to minimize any non-compliance risk and designate the appropriate representative in Korea after considering various factors since the representative is tasked with a very important role.

7.1.2. *Restrictions on Onward Transfers of Personal Information to a Third Country (Amended Act, Article 63(5))*

The current version of the Network Act places certain restrictions on the cross-border transfer of personal information from Korea to an overseas location (Article 63), but does not specifically regulate the onward transfer of the said personal information to a third country after the initial transfer (which the Amended Act does).

(a) Key features of Article 63(5)

(i) Who will be subject to this new provision?: Anyone who receives personal information from a Korean business entity that is subject to the Network Act ("**Third-Party Recipient**").

(ii) Obligations of Third-Party Recipients: Third-Party Recipients (i) may not enter into any data processing agreement that violates the Network Act; (ii) must obtain the user's consent to re-transfer his/her personal information to a third country(yet, if the onward transfer is necessary to perform the contract with the users and enhances the convenience of users, consent does not need to be obtained as long as information concerning the onward transfer is disclosed in the privacy policy); and (iii) must implement certain safeguards prescribed by the Enforcement Decree of the Network Act in order to protect the personal information that is being re-transferred to a third country.

(iii) What happens in case of a violation: If the Third-Party Recipient fails to obtain the user's consent to the onward transfer of his/her personal information, the Third-Party Recipient may be required to pay a penalty surcharge of up to 3% of its relevant revenue. Meanwhile, failure to implement the security measures prescribed by the Enforcement Decree of the Network Act may result in an administrative fine of up to KRW 30 million (about USD 26,000).

(b) Implications of Article 63(5)

The adoption of Article 63(5) is expected to accelerate the ongoing process for the European Commission's adequacy decision regarding the level of data protection offered by Korea. In addition, when it takes effect, Article 63(5) will finally provide a statutory basis for regulating onward transfers of personal information to third countries after initial cross-border transfers from Korea. As such, it will be necessary for Third-Party Recipients (including the foreign affiliates of Korean companies) that receive personal information from Korean ICSPs to check whether they will be conducting onward transfers of such personal information to third countries and the purposes of such transfer in order to ensure compliance with the various requirements contained in this new provision.

7.1.3. *Creation of Reciprocity Provision (Amended Act, Article 63-2)*

(a) Key Features of Article 63-2

It provides that comparable restrictions may be placed on cross-border transfers of personal information to ICSPs of any country that has placed restrictions on cross-border transfers of personal information (excluding cases where cross-border transfers are made pursuant to international treaties or agreements).

(a) Implications of Article 63-2

The creation of this provision appears to be a response to the localization trend affecting the regulation of personal information throughout the world as evidenced by the restrictions placed on cross-border transfers of personal information in certain countries. Specifically, the adoption of Article 63-2 is seen as an attempt by Korean regulators to achieve parity with the regulatory policies of other countries. It enhances the protection of the personal information of Korean data subjects by subjecting foreign ICSPs to similar restrictions on cross-border data transfers as those applying to Korean companies in such countries, at a time when the economic value of personal information is ever increasing. However, Article 63-2 merely provides a possibility that Korean regulators may impose similar restrictions based on the principle of reciprocity, without specifying which regulator will issue such restrictions and which entities or individuals of other countries may actually be subject to such restrictions. Therefore, it appears difficult at the moment to implement specific and meaningful restrictions based on the principle of reciprocity by using this provision alone. Consequently, it may be necessary to keep track of how Korean regulators interpret and enforce this provision after the Amended Act takes effect.

7.1.4. *Conclusion*

Notably, the Amended Act is the first representative system and rules for onward transfers of personal information that has been adopted by Korea's data protection regime. As discussed above, the Amended Act expands the applicability and enforceability of the Network Act to Foreign Service Providers and subjects them to strict restrictions on onward transfers of personal information to third countries after initial cross-border transfers from Korea. In particular, companies actively conducting cross-border data transfers to and from affiliates situated across various jurisdictions are advised to pay special attention to Article 63(5) of the Amended Act. Additionally, the adoption of Article 63-2 of the Amended Act may, depending on the specific measures that will be implemented by Korean regulators, have far-reaching consequences on cross-border transfers of personal information in the future. Therefore, ICSPs and Third-Party Recipients – both with and without a local address or place of business in Korea – are advised to continue monitoring developments related to the enactment of the corresponding Presidential Decree and the enforcement practice of Korean regulators following the effective date of the Amended Act.

8. Thailand

John Fotiadis *(Senior Member), Atherton* (johnf@athertonlegal.com); **Pattarapan Choowa** *(Law Clerk), Atherton* (PattarapanC@AthertonLegal.com).

8.1. *Thailand's New Cryptocurrency Laws*

In August 2013, a Thai company named Bitcoin Co. Ltd. ("**BCL**") asked the Bank of Thailand ("**BOT**") what guidelines and licensing requirements are applicable to their bitcoin operations. In particular, BCL operated a bitcoin exchange in Thailand that handles the purchase and sale of bitcoins. The Ministry of Finance and the BOT conducted meetings with BCL to determine the applicability of current laws to BCL's operations, and to bitcoin transactions in general.

In the absence of any specific legislation, the BOT decided to give BCL some space to operate. The BOT determined that Bitcoin and crypto-currency does not fall clearly within any of the defined "foreign means of payment" under the Exchange Currency Act and could not be prohibited as a matter of law (provided they were not used for foreign exchange).

Five years later, Thailand has forged ahead with new laws authorizing cryptocurrency use, exchange and investment as well as providing rules for operators and a framework for initial coin offerings ("**ICOs**") that have unlocked the potential for significant growth.

The BOT in cooperation with the Ministry of Finance and the Securities and Exchange Commission ("**SEC**") have enacted several integrated laws clearing the road for cryptocurrency and ICOs to proceed, subject to certain registration requirements. The principal law entitled the Royal Decree for Digital Asset Businesses defined cryptocurrencies as part of "digital assets and digital tokens" to be officially regulated by the SEC. It became effective in May 2018.

The new law authorizes domestic operation for cryptocurrency exchanges, brokers and dealers, provided that the operators are Thai companies that have registered with the SEC (effective from August 2018). No license approval is necessary, but operating without being registered can result in fines up to twice the value of the digital transactions conducted or at least THB 500,000 (USD $16,000) and imprisonment of up to two years.

This was followed by new regulations enacted in July 2018, officially authorizing and regulating ICOs. The Digital Asset Management Act authorizes Thai companies with registered capital of at least THB 5 Million (USD $160,000), appropriate management/personnel and an approved business plan with distribution structure, to operate an ICO portal for offerings to institutional investors, high net worth individuals, venture capital and private equity firms.

The SEC has also already approved J Ventures, a subsidiary of Jay Mart PLC, as the first company to raise capital by ICO. J Ventures successfully raised THB 660 Million (USD $2 Million) in 48 hours in the first ICO offering.

The BOT has also backed away from its earlier position barring banks from participating in any cryptocurrency operations. While BOT still prohibits banks and financial institutions from dealing directly in cryptocurrency, it announced on 1 August 2018 that it now allows the industry to issue digital tokens, offer supporting brokerage and related services, and invest in cryptocurrency through bank subsidiaries (provided that such services are not offered to the general public and individuals, but only to other business operators).

The BOT has also announced plans in September 2018 for developing Project Inthanon, its own form of digital currency as a form of government authorized cryptocurrency). Working with eight participating banks, the BOT plans to design and introduce a prototype currency to be used for funds transfers.