Available online at www.sciencedirect.com

ScienceDirect

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

Computer Law & Security Review

Asia Pacific

Gabriela Kennedy

Mayer Brown, Hong Kong

1. China

1.1. *Considering these? App-solutely not! – China issues measures for the identification of illicit collection and use of personal information by apps*

On 30 December 2019, the Cyberspace Administration of China, Ministry of Industry and Information Technology, Ministry of Public Security and State Administration for Market Regulation jointly released the Measures for the Identification of Illicit Collection and Use of Personal Information by Apps ("*Measures*"). The Measures set out negative examples relating to the collection and use of personal information by mobile applications operators ("*App operators*") under specific circumstances, which can be divided into six categories.

Since January 2019, regulators have embarked on a nationwide enforcement campaign ("*Campaign*") against the illicit acquisition and use of personal data by App operators, under China's Cybersecurity Law ("*CSL*") and the Law on Protection of Consumer Rights and Interests. The Campaign focused on excessive data collection forced consent to the use of personal data of users, use of data without consent, failing to remedy cybersecurity breaches and selling or distributing users' data illicitly. The punishments meted out included naming and shaming App operators, and suspending or terminating the App operators' services in more severe cases. Regulators have also highlighted that, besides complying with the CSL and other relevant laws, App operators should also abide by the principles of legality, propriety and necessity, and should not collect personal information that is unrelated to the services provided.

1.1.1. *List of negative examples*

The six categories contained in the Measures have previously been identified as general violations under the CSL, but little to no further details or guidance relating to these categories had been provided. The Measures now offer a list of examples and scenarios relating to each of the six categories. These examples will assist both App operators (when conducting self-assessment) and regulators (when enforcing privacy laws) in determining whether a particular situation would constitute a breach of the CSL and other formal laws. The list of examples is discussed below.

(a) *Failing to publicise the rules of collecting and using personal data*

Examples include: (i) failing to put in place privacy policies or to include rules relating to collecting and using personal information ("Rules") in privacy policies; (ii) failing to bring the privacy policy and Rules to the users' attention by displaying them in a conspicuous way upon the user's initiation of the app, such as through a pop-up window; (iii) setting inaccessible privacy policies; and (iv) setting unreadable privacy policies.

(b) *Failing to clarify the purpose, method, and scope when collecting and using personal data*

Examples include: (i) failing to list the purpose, method, and scope of the collection and use of personal data by the app, including entrusted or embedded third-party codes and plug-ins; (ii) where there are changes to the Rules, failing to notify users via appropriate means of changes to privacy policies and reminding users to read them; (iii) failing to notify users of the purpose of data collection and use or where the purpose is stated in a way that is unclear or difficult to comprehend when applying for authorisation to access a user's ID number, bank account, location, and other sensitive information; and (iv) setting obscure, lengthy and complex rules for collection and use of personal data.

(c) *Collecting or using personal information without obtaining user consent*

Examples include: (i) collecting personal information or activating such authorisation before obtaining user con-

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

https://doi.org/10.1016/j.clsr.2020.105435
0267-3649

sent; (ii) collecting personal information or activating such authorisation beyond the scope of a user's authorisation; (iii) obtaining user consent through non-explicit means such as through default settings; (iv) changing the status of the data collection authorisation without obtaining user consent; and (v) failing to provide users with means to revoke consent to personal data collection.

(d) *Collecting personal data that is unrelated to the services provided by the app*

Examples include: (i) collecting personal information or activating such authorisation that is unrelated to the app's business and functions; (ii) refusing to provide certain functions when users refuse to provide unnecessary information or grant such authorisation; (iii) refusing to provide original functions when users reject new functions that apply to collect information beyond the scope of users' previous consent, except if the new functions replace the original functions; and (iv) collecting personal information at a frequency that exceeds the practical needs of the app's function.

(e) *Providing personal information to others without obtaining user consent*

Examples include: (i) failing to obtain user consent or to anonymise the data collected before providing it to third parties (including embedded third-party codes and plug-ins); (ii) failing to obtain user consent or to anonymise the data before uploading it to background servers and sending to third parties; and (iii) failing to obtain user consent before connecting to third-party apps and sending a user's personal data.

(f) *Failing to provide the function of amending or deleting personal data according to laws and regulations or failing to publish complaint or reporting channels*

Examples include: (i) failing to provide valid functions for users to amend or delete their personal information or cancel their accounts; (ii) imposing unnecessary or unreasonable conditions on users who wish to amend or delete their personal information or cancel their accounts; (iii) failing to complete verification and processing procedures within 15 working days, or within a prescribed period not exceeding 15 working days, where manual handling is required to amend or delete users' personal information or to cancel their accounts; and (iv) failing to establish and publish personal information security complaint and reporting channels, or failing to handle complaints within 15 working days or within a prescribed period not exceeding 15 working days.

1.1.2. Potential implications

The publication of the Measures is a beneficial step to both App operators and regulators. From a compliance point of view, App operators have greater clarity, particularly when conducting their self-assessment, on how to comply with the CSL and other privacy-related laws through specific "negative" examples that they should do well to avoid. From an enforcement angle, the Measures act as a reference for regulators enforcing privacy laws to determine whether a situation (such as instances of illicit collection and use of personal data by apps) would constitute a breach of the CSL and the related regulations and guidelines. As a whole, the Measures will guide public supervision and strengthen the implementation of privacy-related laws in China.

Although these Measures are not strictly legally binding, the Chinese regulators have been known to apply guidelines as an important measure of compliance with China's formally binding data protection rules, including those contained in the CSL. Therefore, to minimise the risk of non-compliance with the CSL, organisations are recommended to comply with these standards as far as practicably possible if they are operating or intend to operate a mobile application in China.

Gabriela Kennedy (Partner), Mayer Brown
(gabriela.kennedy@mayerbrown.com);
Cheng Hau Yeo (Associate), Mayer Brown
(chenghau.yeo@mayerbrown.com);
Samantha A. Cheung (Intellectual Property Officer), Mayer Brown
(samantha.cheung@mayerbrown.com).

2. Hong Kong

2.1. *Out with the old, in with the new: proposal for review of the personal data (privacy) ordinance*

Enacted in 1995 and in force since 1996, the Hong Kong Personal Data (Privacy) Ordinance (Cap. 486) ("*PDPO*") is one of the earliest data privacy laws in Asia. It was last amended in 2012, with the most notable change being the introduction of direct marketing regulations that came into force in April 2013. While data protection regimes around the world have evolved in recent years to meet the demands of the digital age, the PDPO has not been amended since 2012. Once considered pioneering, the PDPO is now at risk of falling behind and being out of step with international developments.

After much anticipation, the Constitutional and Mainland Affairs Bureau ("*CMAB*") and the Privacy Commissioner for Personal Data ("*PCPD*") released a paper (LC Paper No. CB(2)512/19-20(03)) ("*Paper*") proposing amendments to the PDPO. The Paper was discussed at the meeting of the Legislative Council Panel on Constitutional Affairs ("*Panel*") on 20 January 2020 ("*Meeting*").

While no major overhaul of the PDPO has been proposed, the Paper sets out six recommended amendments. Some of these amendments are direct responses to recent events in Hong Kong which have highlighted inadequacies in the data privacy legislation, such as the prevalent practice of doxxing (i.e. the unauthorised disclosure of personal data as a means of harassment or intimidation) used during the Hong Kong protests in 2019. Other proposed amendments, such as the mandatory breach notification, are a nod in the direction of international developments.

Key recommendations

2.1.1. *Mandatory data breach notification*

Currently, Data Protection Principle ("*DPP*") 4 of the PDPO provides that data users must take all practicable steps to prevent unauthorised or accidental access to personal data. There is no mandatory notification requirement to the PCPD or the affected data subjects in the event of a breach regardless of its severity, although the Guidance on Data Breach Handling and the Giving of Breach Notifications issued by the PCPD in 2010 (last revised in 2019) recommends that voluntary notifications be made where data subjects can be identified and there is a reasonably foreseeable risk of harm arising from the data breach.

Given the rising number of data breaches in Hong Kong and internationally, the adequacy of the voluntary notification system has been called into question. More often than not, the PCPD and affected individuals are only notified of a data breach when it hits the headlines, and this may likely hinder timely follow-up actions.

At the same time, mandatory data breach notifications have become the international norm – Australia, Canada, China, the EU, the Philippines, South Korea and Taiwan have all put in place a mandatory notification system, and Singapore and New Zealand are expected to roll out such a system shortly. In the previous review of the PDPO, the government chose not to implement a similar proposal given that the mandatory notification system was in its infancy. It is now, however, opportune for Hong Kong to re-evaluate its position.

The Paper proposes the adoption of a mandatory data breach notification system influenced by international concepts including the introduction of: (a) a definition of 'personal data breach'; (b) a notification threshold; (c) a timeframe for notification; and (d) a format for the notification. These elements are discussed below:

(g) *The definition of "personal data breach"*

> In line with the definition of the General Data Protection Regulation ("GDPR"), a "personal data breach" is defined as: "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*".

(h) *The notification threshold*

> Data users are required to make notifications for data breaches with "*a real risk of significant harm*". The CMAB and the PCPD are studying whether to apply the same threshold for making notifications to the PCPD and affected data subjects.

(i) *The timeframe for notification*

> Data users are required to make notifications within a specified timeframe (e.g. no later than five business days after the data user becomes aware of a breach). The CMAB and the PCPD are also considering whether a specified period may be added for data users to investigate and verify the data breach before making a notification.

(j) *The method of notification*

> Data users shall make notifications via email, fax or post. Certain information, such as a description of the data breach, an assessment of the risk of harm and the type and amount of personal data involved, should be included in the notification.

A few of the elements for the mandatory breach notification had led to a debate amongst members of the Panel. Further clarification as to the meaning of "*real risk of significant harm*" was requested. Indeed, how the notification threshold is defined is an essential point – while breach notifications may enable the PCPD and affected individuals to take prompt follow-up actions, the risk of "over-notification" should also be borne in mind – an unduly low threshold would not only be costly to both data users and the PCPD, but may also lead to data subjects being bombarded with untimely breach notifications unnecessarily. The timeframe of notification should also be carefully defined to allow time for companies to assess the situation and make meaningful notifications. The five business day timeframe suggested in the Paper appears to be more generous than the 72-h deadline in the GDPR. However, the GDPR's stricter deadline is mitigated by allowing notifications to be done in phases (as long as this is done without undue further delay) and permitting a delayed notification where a reasoned justification can be given.

Finally, it must be borne in mind that the mandatory notification system only works if similar requirements also apply to data processors, given the high volume of data that is entrusted to data processors and the fact that most data breaches see the involvement of a data processor in one way or another. Under the GDPR, the mandatory breach notification applies to data processors alike and they must promptly inform the relevant data controllers. Sensibly, the Paper proposes a similar (and possibly stricter) requirement under which data processors may also be required to notify the PCPD in addition to the relevant data users.

2.1.2. *Data retention policies*

At present, DPP2 of the PDPO requires data users to take all practicable steps to ensure that personal data is not kept longer than necessary for the fulfilment of the purpose for which the data is to be used (or a directly related purpose). It does not specify any retention periods for personal data. However, the PCPD has issued guidelines on the retention periods of specific types of personal data. For instance, the PCPD recommends that employers should not retain the personal data of former employees for more than seven years after the end of the employment, unless there is a subsisting reason to hold the data for a longer period or if the data is necessary for employers to comply with contractual or legal obligations (e.g. taxation requirements).

The Paper notes that it is impractical to prescribe a uniform retention period for all types of data held for different purposes. Instead the Paper introduces a requirement that data users lay down a clear retention policy which addresses information such as the maximum retention periods for different categories of personal data, the legal requirements which may affect the designated retention periods, and how the retention

period is calculated. The Paper further proposes requiring data users to make their data retention policies public.

The recent case of the disclosure of data in the inactive customer database of a telecommunications company is a salutary reminder that retaining personal data for longer than necessary often leads to a heightened risk of a data breach. A requirement to establish and disclose data retention policies will help bolster data users' accountability and transparency with respect to data retention.

2.1.3. *Direct regulation of data processors*

Unlike the data privacy laws in other jurisdictions such as the EU, Australia, Canada, New Zealand and Singapore, the PDPO does not directly regulate data processors. Data users are obliged to adopt contractual means to ensure their data processors comply with data security and retention requirements, and are ultimately liable for any acts or omissions of their data processors which are in contravention to the law. The Paper proposes that the PDPO directly impose obligations on data processors in order to strengthen the protection of personal data and ensure a fair apportionment of responsibilities between data users and data processors.

Indeed, as seen from data breaches which arose at the data processor level, data users may only exert limited influence over data processors through contractual means, and it may be difficult to request the cooperation of data processors in mitigating the damage done in a data breach. Direct regulation, on the other hand, allows data processors to be held equally accountable as data users, and enables data subjects to bring claims against data processors in addition to claims against data users.

Lobbying on the part of data processors is to be expected and they will no doubt argue that in most cases they do not possess knowledge of the nature of the data entrusted, and certain obligations under the PDPO should not apply to them. It may be more reasonable to require data processors to comply with specific requirements such as data retention and security obligations and the requirement to make data breach notifications to data users, as suggested in the Paper. These obligations appear less extensive than the obligations imposed on data processors under the GDPR, which also requires data processors to maintain records of their processing activities and appoint data protection officers, etc. In any case, the details of the proposed amendments would have to be refined to fit local circumstances and consultation with relevant stakeholders, especially the IT sector, is important to understand the potential operational difficulties of data processors in complying with various requirements under the PDPO.

2.1.4. *Expanded definition of personal data*

The Paper proposes the expansion of the current definition of personal data (i.e. data relating to an "identified" person) to cover data relating to an "identifiable" person. This means that a piece of information will be "personal data" as long as it is reasonable to expect that such piece of information may be used (alone or in combination with other information) to directly or indirectly identify a person. The effect of this change will be that online identifiers (e.g. IP addresses) and online behavioural analytics will fall within the definition of personal data and will align the PDPO with the position in other jurisdictions such as the EU, Canada, Australia and New Zealand.

2.1.5. *Regulation of doxxing*

Since June 2019, the PCPD has focused his attention on enforcement actions against doxxing activities. According to the Paper, the PCPD's office has handled over 4700 doxxing cases since 14 June 2019 and has referred more than 1400 cases to the police for criminal investigation.

At present, data users who engage in doxxing may be in contravention of DPP1 (for collecting personal data through unlawful or unfair means), DPP3 (for using personal data for a new purpose without consent) and be guilty of an offence under section 64 for disclosing personal data obtained from another data user without such data user's consent and thereby causing psychological harm to the data subject. However, the PCPD has encountered major obstacles in countering doxxing activities, especially due to his lack of power to compel online platforms (data processors) to remove doxxing posts and to initiate the conduct of criminal investigations himself in such cases.

To more effectively curb doxxing activities, the Paper recommends the introduction of amendments that specifically address doxxing, conferring the PCPD with the statutory power to order online platforms to remove doxxing content, undertake criminal investigations and initiate prosecutions for doxxing cases.

This proposal was the focus of the Panel's discussion at the Meeting, and members were generally supportive of the idea of giving the PCPD more "teeth" in tackling doxxing. In fact, the PCPD's office has been described as a "toothless tiger" for years. This is not the first time the PCPD asked for enhanced powers. In the review of the PDPO in 2009, the PCPD pushed for the introduction of new powers in the PCPD to include criminal investigations and prosecution powers.

Meanwhile, in formulating rules to tackle doxxing, it is key to maintain a clear line between harmful doxxing behaviour and, for instance, legitimate news activities involving the disclosure of a public figure's personal data in the public interest. The CMAB and the PCPD are expected to draw insights from the legislative and regulatory experience of New Zealand which passed a similar law to combat doxxing in 2015, and Singapore which recently introduced a bill to similar effect.

2.1.6. *Increased penalties*

Currently, the PCPD is not empowered to impose an administrative fine, but he can only issue an enforcement notice directing data users to take remedial steps in the event of a contravention of one of the DPPs. It is only when a data user fails to comply with an enforcement notice that he commits an offence and is liable, on first conviction, to a fine up to HK$50,000 and imprisonment for two years (and a daily fine of HK$1000 if the offence continues). However, so far, Hong Kong courts have only issued fines between HK$1000 to HK$5000 for cases of non-compliance with enforcement notices.

This stands in stark contrast to the practice elsewhere. The GDPR, for instance, empowers regulatory authorities to levy administrative fines of up to €20 million or 4% of the organisation's annual global turnover, whichever amount is higher. In January 2019, the French data protection authority, CNIL,

issued a fine of €50 million against Google for a number of infringements under the GDPR. In July 2019, the UK's Information Commissioner's Office (ICO) proposed a fine of £183 million for British Airways following a data breach involving around 500,000 of its customers, and a £99.2 million fine for Marriott International following a hack involving the personal data of over 339 million of its guests.

In order to really become a law that has a deterrent effect, the Paper proposes increasing the levels of fines and conferring the PCPD with the power to issue administrative fines for violations of the PDPO, if a certain threshold is met (determined by a number of factors e.g. the type of data compromised and the intent of the data user). Drawing reference from the GPDR, the Paper also suggests linking the amount of the administrative fines to the annual turnover of data users.

Enhanced penalties, especially the power of the PCPD to issue administrative fines, will serve to escalate data privacy issues to the board level and reinforce the protection of personal data. Meanwhile, compliance costs will certainly increase for businesses. The threshold for issuing administrative fines and the maximum amount of such fines should be cautiously calibrated with reference not only to overseas regulatory experience, but also the local circumstances of Hong Kong.

More proposed reforms to come?

Certain members of the Panel criticised the proposed amendments as being inadequate. In fact, when benchmarked against the GDPR and the data privacy laws of other jurisdictions, it is clear that certain key elements are missing from the Paper. For instance, many jurisdictions, such as the EU and Australia, distinguish between "sensitive personal data" (e.g. biometric data, medical data, financial data) and "personal data" and have laid down more stringent requirements with respect to sensitive personal data. This point was not addressed in the Paper.

What is also surprising is the absence of any mention of cross-border data transfer restrictions in the Paper. While section 33 of the PDPO provides that personal data may only be transferred outside Hong Kong (including the PRC) under specified conditions, this section is the only section in the PDPO which has yet to be brought into force. During the Meeting, the PCPD clarified that there is currently no timetable for bringing the long overdue section 33 into force, but his office will consider implementing section 33 after further guidelines on cross-border data transfer are issued in the first half of 2020.

Proposals relating to enhanced rights of data subjects under the GDPR, such as the right to object to processing, the right not to be subject to automated decision making (including profiling) and the right to be forgotten are also missing from the Paper. The PDPO currently does not provide data subjects with any of these rights.

What's next?

The discussion of the Paper at the Meeting is just the beginning of the PDPO's review process. The CMAB and the PCPD are expected to conduct further studies on the proposed amendments and consult with relevant stakeholders before introducing a formal amendment bill into the Legislative Council. Legislative amendments do not happen often. This is a golden opportunity to bring our data protection legislation in line with international developments in order to maintain Hong Kong's competitiveness as an international data hub.

No timetable has been set for the proposed amendments though the Secretary for CMAB made it clear that no public consultation would be held in order to streamline the review process.

Conclusion

The Paper is a step in the right direction, seeking to align Hong Kong's data privacy laws with international standards and respond to local data privacy incidents in recent years. Nonetheless, the devil is in the detail and the Paper departs from international norms by missing out certain key elements such as cross-border data transfer restrictions. Any amendment to the PDPO should aspire to be comprehensive, particularly if Hong Kong wishes to obtain an adequacy decision from the European Commission and bolster its competitiveness in terms of international data flows. However, given that the Paper only sets out "preliminary recommendations", it may mean that the final amendment bill would present a more holistic and proactive overhaul of the legislation.

In the meantime, it is crucial for companies in Hong Kong to closely track the developments of the review of the PDPO, assess the impact of the proposed amendments on their business operations and carry out preparations early on.

Gabriela Kennedy (Partner), Mayer Brown (gabriela.kennedy@mayerbrown.com);
Cheng Hau Yeo (Associate), Mayer Brown (chenghau.yeo@mayerbrown.com);
Christopher C. H. Ng. (Trainee Solicitor), Mayer Brown (christopher.ng@mayerbrown.com).

3. Japan

3.1. *Japanese copyright act set for revision*

3.1.1. *Introduction*

On 10 March 2020, the Japanese government approved a bill to revise the Copyright Act ("*Revised Bill*") containing strengthened measures against pirated sites on the Internet, and submitted it to the National Diet.

Under the current Copyright Act, it is illegal to upload copyright work to the Internet without the copyright owner's permission. However, in relation to illegal downloading, only music and video downloads are prohibited. In 2019, the Agency for Cultural Affairs drafted an amendment to the Copyright Act to expand the scope of illegal downloading through pirated sites. However, the proposed amendments faced strong opposition from various stakeholders who invoked freedom of expression concerns. In response to such public opposition, the Liberal Democratic Party withdrew the bill and the proposed amendments were subsequently refined by the Agency for Cultural Affairs and introduced through the Revised Bill.

The Revised Bill includes: (a) the strengthening of anti-piracy measures on the Internet; and (b) other matters.

3.1.2. *Strengthening anti-piracy measures on the Internet*

The cartoon and magazine industries have been heavily affected by pirated sites. For example, it has been estimated that approximately 300 billion JPY (approximately 2.7 billion USD)

worth of cartoons have been illegally accessed through a pirated cartoon site "Manga Mura" for free, resulting in cartoon artists and publishers losing 20% in revenue and sales. It has also been estimated that approximately 73 billion JPY (approximately 0.7 billion USD) worth of damages have been caused by "leech websites" that provide users with links to download pirated copyright work. A survey has shown that any infringing content uploaded without the copyright owner's permission can be viewed about 62 times more frequently when a link is attached to the "leech website". In order to protect the creative content industry, the Revised Bill sets out regulations in relation to: (a) "leech websites"; and (b) the downloading of illegal content.

(a) *Regulation of "leech websites"*

Under the Revised Bill, the act of operating "leech websites" and "leech applications" will be subject to criminal penalties, under which an imprisonment for up to 5 years or a fine of up to 3 million JPY may be imposed. The posting of a link to infringing content on a leech website will also be made illegal and the person responsible for posting the link will be subject to civil and criminal liabilities.

(b) *Regulation of downloading of illegal content*

Under the Revised Bill, the scope of restrictions on downloading illegally uploaded works will be expanded to cover all copyright works including cartoons, books, and computer programs. However, to avoid the excessive curtailment of rights relating to the collection of information, the regulations will only apply to users downloading data with the knowledge that it was illegally uploaded. In addition, the following actions will be excluded from regulation:

(i) minor acts such as downloading up to several frames from tens of pages of comics;
(ii) downloading secondary works and parody; and
(iii) if the download falls within a special situation that does not unduly impair the interests of the copyright owner. For example, the exception applies where a manual on how to deceive people is created by a fraudulent crime group and posted on a whistle-blowing site by a group of victims without the fraudulent crime group's permission, and such manual is downloaded for the purpose of protecting an individual and his or her family.

Criminal penalties will only be imposed for particularly malicious acts. In particular, repeated downloading of a copyright work for which a regular version is provided for a fee will be punished with imprisonment for up to 2 years or a fine of up to 2 million JPY.

3.1.3. Other matters

Under the Revised Bill, measures allowing fair use of copyright works will be introduced. For example, under the current Copyright Act, copying an unexpected appearance of something unwanted when taking a photograph or recording is allowed, and under the Revised Bill, these exceptions will be extended to the copying of such unexpected appearance when taking a screenshot or conducting live streaming on the Internet.

Furthermore, additional measures will be introduced to ensure appropriate protection of copyright. Under the current Copyright Act, in a copyright infringement action, the court may issue a document submission order to the defendant who owns the necessary documents required for proving infringement or calculating the amount of damage. However, the court is not allowed to review the actual documents before determining whether it is necessary to issue a submission order. Under the Revised Bill, the court will be able to review the actual documents before it determines whether it is necessary to issue a document submission order, and the court will be able to receive the support of expert advisors (such as university professors) when assessing the necessity of a document submission order.

Lastly, a new registration system for copyright work will also be established under the Revised Bill.

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

4. New Zealand

4.1. *Privacy bill – current status*

The Privacy Bill, which is intended to replace the Privacy Act 1993, is currently tabled before the Committee of the Whole House in Parliament. During this stage, Members of the Parliament will have the chance to debate the Privacy Bill in detail and propose amendments before the third reading of the Privacy Bill.

4.1.1. Supplementary order paper

On 17 March 2020, the Justice Minister released a Supplementary Order Paper ("SOP") with what is anticipated to be the final suite of changes to the Privacy Bill. The Parliament will debate this SOP in the coming months.

4.1.2. SOP amendments to the privacy bill

The Privacy Bill, as introduced into Parliament on 20 March 2018, proposes several key reforms to the Privacy Act including:

(a) mandatory data breach reporting;
(b) higher enforcement powers for the Privacy Commissioner;
(c) increased fines (up to NZ$10,000);
(d) the creation of new criminal offences; and
(e) the strengthening of cross-border data flow protection.

4.1.3. Timing

The Privacy Bill was previously scheduled to come in force on 1 March 2020. That deadline has passed and the new commencement date proposed in the SOP is 1 November 2020 (except for a few regulation-making powers which will come into

force the day after the new Privacy Act passes). This new deadline presents a window of opportunity for businesses to proactively ensure their privacy policies and processes are fit for purpose.

4.1.4. *Greater clarity on extraterritorial effect*
Amendments included in the SOP make it clear that the new Privacy Act will apply to:

(a) any action taken by a New Zealand agency in respect of personal information collected or held by that agency – whether or not the action was taken while the agency was present in New Zealand;
(b) any action taken by an overseas agency in the course of carrying on business in New Zealand in respect of personal information collected or held by that agency; and
(c) any action taken by an individual not ordinarily resident in New Zealand in respect of personal information:
    (i) collected by the individual while in New Zealand (regardless of where the information may be subsequently held or where the subject of the information is located); and
    (ii) held by the individual while present in New Zealand (regardless of where the subject of the information is located).

While the SOP extends the application of the new Privacy Act to overseas agencies carrying on business in New Zealand, the Privacy Bill does not provide a definitive definition of what would constitute "carrying on business in New Zealand" for the purposes of the new Privacy Act. What the Privacy Bill does provide is that an agency may be treated as carrying on business in New Zealand without necessarily:

(a) being a commercial operation;
(b) having a place of business in New Zealand;
(c) receiving any monetary payment for the supply of goods or services; or
(d) intending to make a profit from its business in New Zealand.

It is likely that whether or not an overseas agency is carrying on business in New Zealand will be a matter to be assessed on a case by case basis, and very fact dependent.

4.1.5. *Notifiable privacy breach and compliance*
Under the Privacy Bill a notifiable privacy breach is a privacy breach that is reasonably believed to have caused, or to be likely to cause, serious harm to the affected individual(s). Notice of notifiable privacy breaches is required to be given to the Privacy Commissioner and the affected individual(s) as soon as practicable after becoming aware that the breach has occurred. The agency concerned may also be required to provide the affected individuals with identifying details of any person in possession of their information if the agency concerned believes, on reasonable grounds, that such disclosure is necessary to prevent or lessen a serious threat to life or health to the affected individual or another person.

New clauses have also been added, which relate to the liability of employers and members of agencies. These clauses make it clear that employees or members of agencies will not be personally liable if their actions result in an employer or agency failing to notify a privacy breach. Only employers and agencies will be liable for such breaches.

4.1.6. *Children and young persons*
The SOP has added a requirement that an agency must ensure that the means of collection of personal information are fair and not unreasonably intrusive, particularly when collecting personal information from children and young persons.

4.1.7. *Complaints, proceedings and class actions*
The SOP provides that any person may make a complaint on behalf of one or more aggrieved individuals. The representative complainant does not need to be the aggrieved individual. Proceedings in the Human Rights Review Tribunal may also be commenced by a representative of a class of aggrieved individuals. The Tribunal may award damages to each member of a class of aggrieved individuals.

4.1.8. *Sharing, accessing and matching personal information*
An agency that enters into an information sharing agreement to facilitate the provision of public services must now be named as a party to the agreement. Only a specified agency (i.e. a public sector department, part of a public sector agency, or a specified Crown entity) may be the lead agency in an information sharing agreement, and the Privacy Commissioner may review the agreement (with permission of the Minister) within 12 months.

4.1.9. *What next?*
There is no indication yet as to when the third reading of the Privacy Bill might occur, but it is anticipated that it will be passed as it has the support of both the Government and the opposition, and the Office of the Privacy Commissioner is anticipating a six month period between the passing of the Privacy Bill and the commencement of the new Privacy Act.

Karen Ngan (Partner), Simpson Grierson (karen.ngan@simpsongrierson.com);
Maddy Rowe (Solicitor), Simpson Grierson (maddy.rowe@simspongrierson.com);
Maria Nieto (Solicitor), Simpson Grierson (maria.nieto@simspongrierson.com);
Po Tsai (Solicitor), Simpson Grierson (po.tsai@simpsongrierson.com).

4.2. *Films, videos, and publications classification (commercial video on-demand) amendment bill – current status*

The Films, Videos, and Publications Classification (Commercial Video on-Demand) Amendment Bill ("*CVoD Bill*") was introduced before Parliament on 10 December 2019 and is currently at the Select Committee stage. During this stage, the Select Committee normally calls for public submissions, hears evidence on those submissions, and recommends amendments to the House.

4.2.1. *Objective of the CVoD bill*

The objective of the CVoD Bill is to reduce the potential for harm to consumers from viewing inappropriate content. It proposes amendments to the Films, Videos, and Publications Classification Act 1993 ("*Act*") to ensure consumers see more consistent ratings and descriptive notes across the main commercial (subscription and transactional) video on-demand ("*CVoD*") content platforms in New Zealand.

Currently in New Zealand, providers of CVoD content are displaying inconsistent ratings and descriptive notes, or no ratings at all, for content available on their platforms. There have been differences of opinion on whether or not on-demand online content in New Zealand is currently subject to mandatory rating requirements in the same manner as films for cinematic or DVD release.

4.2.2. *New requirements proposed in the CVoD bill*

Specified providers will need to label the CVoD content they provide in New Zealand. This means following the current process under the Act for rating and labelling of a film, or self-rating content using systems that have been approved by the Office of Film and Literature Classification ("*Classification Office*"). Once the content is labelled, that label must be used by any other specified provider providing that content.

4.2.3. *Which CVoD content providers are regulated*

Specified providers required to comply with the amendments in the CVoD Bill, to the extent that they make CVoD content available in New Zealand, are listed in a schedule to the CVoD Bill. The entities currently listed in the schedule are: (a) Alphabet Inc; (b) Amazon.com, Inc.; (c) Apple Inc.; (d) Lightbox New Zealand Limited; (d) Microsoft Corp.; (e) Netflix, Inc.; (f) Sky Network Television Limited; (g) Sony Interactive Entertainment Europe Limited; and (h) The Walt Disney Company.

Additionally, subsidiaries or affiliated companies of the above entities are also regulated to the extent that they make CVoD content available in New Zealand.

The schedule of specified providers is subject to change from time to time. The CVoD Bill also proposes to have extra-territorial effect in relation to specified providers which are overseas companies.

The CVoD Bill does not at this stage extend to user-generated content (such as content that users of sites such as YouTube and Facebook might upload). The Department of Internal Affairs ("*Department*") noted in its Regulatory Impact Statement that including user generated content within the scope of the proposed amendments would be complex, and would raise issues including the need to consider freedom of speech principles under the Bill of Rights Act 1990. The Department's comments indicate that while the classification of user generated content is not currently proposed, it may be considered in the future when there is more time to consider these matters such as freedom of speech.

4.2.4. *Practical implications of the CVoD bill*

Specified providers and any other CVoD content providers considering making CVoD content available in New Zealand will need to be prepared for compliance when new requirements are introduced.

Content, other than objectionable content, will be required to be rated under, and in accordance with, a self rating tool. The self rating tool can be either the relevant specified provider's own self rating system that has been approved by the Chief Censor, or the CVoD online rating tool provided by the Classification Office. Objectionable content will need to be submitted to the Classification Office for classification.

Specified providers should be assessing current content catalogues to identify what has already been rated/classified under the Act, and what has not. All content rated/classified under the Act should be labelled according to the applicable rating/classification. For all other content, specified providers should be ready to label that content in accordance with the rating generated by the self rating tool the specified provider uses.

If a specified provider is considering using its own self rating system, it will need to get ready to apply for approval of the system.

Karen Ngan (Partner), Simpson Grierson (karen.ngan@simpsongrierson.com);
Maddy Rowe (Solicitor), Simpson Grierson (maddy.rowe@simspongrierson.com);
Maria Nieto (Solicitor), Simpson Grierson (maria.nieto@simspongrierson.com);
Po Tsai (Solicitor), Simpson Grierson (po.tsai@simpsongrierson.com).

5. Singapore

5.1. *Launch of the second edition of model artificial intelligence governance framework*

Building on the first edition of the Model Artificial Intelligence Governance Framework ("*Model Framework*") published on 23 January 2019, the Personal Data Protection Commission ("*PDPC*") released the second edition of its Model Framework on 21 January 2020 to provide clearer guidance to organisations on how to deal with ethical and governance issues when deploying artificial intelligence ("*AI*") solutions.

5.1.1. *Background of the model framework*

The Model Framework was first launched in 2019 to provide a voluntary accountability-based framework for adoption by organisations who adopt and implement AI solutions in their operations, and in particular, assist organisations to:

(a) build consumer confidence in the adoption of AI through organisations' responsible use of such technologies to mitigate different types of risks in AI deployment; and
(b) demonstrate reasonable efforts to align internal policies, structures and processes with relevant accountability-based practices in data management and protection, e.g. the Personal Data Protection Act (No. 26 of 2012) ("PDPA") and OECD Privacy Principles.

The Model Framework aims to promote trust and understanding in the use of AI technologies by reference to the following guiding principles:

(a) organisations using AI in decision-making should ensure that the decision-making process is explainable, transparent and fair. Although perfect explainability, transparency and fairness are impossible to attain, organisations should strive to ensure that their use of AI is undertaken in a manner that reflects the objectives of these principles; and
(b) AI solutions should be human-centric. As AI is being used to amplify human capabilities, the protection of the interests of human beings, including their well-being and safety, should be the primary considerations in the design, development and deployment of AI.

5.1.2. *Key updates in the second edition*

Building on the first edition of the Model Framework, the second edition of the Model Framework has sought to include additional considerations (such as robustness, reproducibility, and auditability) and refine the original Model Framework for greater relevance and usability.

The key changes are:

(a) *New measures*

The updated Model Framework now includes three new measures that organisations can employ to enhance the transparency of the algorithms found in AI models, thereby contributing towards building trust in the AI system. These include:

(i) *Robustness* – i.e. the ability of a computer system to cope with errors during execution and erroneous input, assessed by the degree to which a system or component can function correctly in the presence of invalid input or stressful environmental conditions;
(ii) *Reproducibility* – i.e. the ability of an independent verification team to produce the same results using the same AI method based on the documentation made by the organisation; and
(iii) *Auditability* – i.e. the readiness of an AI system to undergo an assessment of its algorithms, data and design processes.

(b) *Other clarifications*

The updated Model Framework also provides other additional section-specific clarifications, which include:

(i) clarifying the concept of "human-over-the-loop" by explaining the monitoring or supervisory role to be performed by a human, with the ability for the human to take over control when the AI model encounters unexpected or undesirable events in AI-augmented decision-making;
(ii) clarifying that organisations can consider factors such as the nature of harm (i.e. whether the harm is physical or intangible in nature), reversibility of harm (i.e. whether recourse is easily available to the affected party) and operational feasibility in determining the level of human involvement in an organisation's decision-making process involving AI; and
(iii) providing suggestions as to the level of information to be provided to customers and/or obtained from AI solution providers when interacting with various stakeholders to build trust in the stakeholder relationship strategies when deploying AI.

(c) *Inclusion of industry examples*

The updated Model Framework now also includes industry examples in each of the four sections, demonstrating effective implementation of the AI governance practices in the respective sections.

(d) *Additional tools to augment the model framework*

In addition to the Model Framework, the following documents have also been concurrently released to guide organisations in the adoption of the Model Framework:

(i) the Implementation and Self-Assessment Guide for Organisations ("ISAGO"), which was jointly developed by the PDPC, Infocomm Media Development Authority and the World Economic Forum Centre for the Fourth Industrial Revolution, was designed to be a companion to complement the Model Framework to help organisations assess the alignment of their AI governance processes with the Model Framework, identify potential gaps in their existing processes and address them accordingly; and
(ii) the Compendium of Use Cases, which sets out various case studies of organisations that have operationalised the Model Framework principles, and was intended to complement the Model Framework by demonstrating how local and international organisations across different sectors and sizes have implemented or aligned their AI governance practices with all sections of the Model Framework.

5.1.3. *Comment*

The second edition of the Model Framework provides additional considerations that organisations may have in implementing AI governance policies and more explicit examples of best practices that can be implemented to ensure responsible governance practices. Given the increasing prevalence of AI solutions, the updated Model Framework is a welcome development that will provide even greater practical guidance to organisations seeking to adopt the Model Framework when deploying AI solutions.

Lam Chung Nian (Partner), WongPartnership LLP (chungnian.lam@wongpartnership.com);
Kenji Lee (Associate), WongPartnership LLP (kenji.lee@wongpartnership.com).

5.2. *IMDA launches internet of things cyber security guide to help enterprise users and vendors secure internet of things systems*

On 13 March 2020, the Infocomm Media Development Authority ("IMDA"), in consultation with the Cyber Security Agency,

launched a new Internet of Things ("*IoT*") Cyber Security Guide ("*Guide*") to provide enterprise users and their vendors practical guidance on how to address the cybersecurity aspects of IoT systems in the acquisition, development, operation and maintenance of these systems. The Guide also contains threat-modelling and vendor disclosure checklists for vendors and users, an explanation of fundamental concepts on which the Guide is based, and a case study to demonstrate how the recommendations can be applied.

In particular, the Guide is targeted at three primary groups:

(a) IoT developers, such as solution architects and programmers, who design, develop and deploy secure IoT products and systems;
(b) IoT providers, such as network operators and platform providers, who need to roll-out, configure, operate, maintain and de-commission IoT systems securely; and
(c) IoT users who want to procure and interact with IoT systems.

The Guide introduces four IoT security design principles and provides a set of baseline recommendations concerning the implementation and operational phases of IoT systems, i.e.:

(a) *Secure by defaults:* making secure choices and ensuring proper configurations (e.g. minimising attack surfaces and system hardening);
(b) *Rigour in defence:* careful consideration and thoroughness in securing IoT systems (e.g. system compartmentalisation and vulnerability assessment/penetration testing);
(c) *Accountability:* controlled access to the IoT systems and proper management of access throughout the system lifecycles (e.g. ensuring the segregation of duties and protecting audit trails); and
(d) *Resiliency:* being prepared for and having the ability to recover from security breaches (e.g. managing vulnerability and regular backup and recovery).

5.2.1. *Implementation phase*

Baseline security recommendations for IoT users and IoT developers during the implementation phase include:

(a) *Secure by defaults*
  (i) *Employ strong cryptography:* Ensure that products/solutions employ current and industry-accepted cryptographic techniques and best practices.
  (ii) *Protect impactful data:* Check impactful data (i.e. keys, credentials, etc.) for authenticity and protect from disclosure and modifications by unauthorised parties.
(b) *Rigour in defence*
  (i) *Conduct threat modelling:* Conduct threat modelling at the start of the implementation phase and account for the intended usage of IoT devices within defined operating environments.
  (ii) *Establish Root-of-Trust*: Establish and utilise Root-of-Trust in key system components as they may host sensitive data and execute impactful operations.
  (iii) *Employ secure transport protocols:* Employ proven transport protocols with security controls properly activated, wherever possible.
(c) *Accountability*
  (i) *Enforce proper access controls:* Enforce proper cyber and physical access controls for devices, networks and data.
  (ii) *Provide audit trails:* Ensure that all attempts to access sensitive data and alter system resources are properly monitored and logged.
(d) *Resiliency*
  (i) *Guard against resource exhaustion:* Ensure that the system employs mechanisms to protect against malicious attacks.

5.2.2. *Operational phase*

Baseline security recommendations for IoT users and IoT providers during the operational phase include:

(a) *Secure by default*
  (i) *Use strong credentials*: Ensure that strong credentials are used, and that password complexity adheres to regulatory requirements or published international best practices.
(b) *Rigour in defence*
  (i) *Segment IoT and enterprise networks:* Employ network segmentation so that IoT devices belonging to different networks can be properly segmented from one another.
(c) *Accountability*
  (i) *Establish proper device management:* Establish proper management of devices, and strictly enforce access controls. IoT users and providers should also subscribe to notifications and advisories issued by the IMDA.
(d) *Resiliency*
  (i) *Recover from attacks*: Conduct regular backups of system data as well as regular disaster recovery exercises for systems.
  (ii) *Conduct periodic assessments:* Conduct penetration testing and/or vulnerability assessments (including threat modelling) of the IoT system periodically.

Additionally, the Guide includes recommendations on identifying and mitigating threats and vulnerabilities posed by IoT systems:

(a) *Security Impact categories*

provides security impact categories for the identification of assets of interest based on impacts to security properties – namely, Confidentiality, Integrity and Availability.

(b) *Threat categories for identifying assets of interests*

identifies six threat categories of a typical IoT solution – namely, Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege;

(c) *Attack surface categories*

identifies the attack surface categories common to IoT devices; and

(d) *Threat assessment*

provides a framework for how threats to an asset may be assessed.

5.2.3. *Comment*

As technology continues to develop, many organisations are embracing the use of IoT systems and devices to increase productivity and build new connected "smart" applications. While there are considerable benefits in using IoT systems and devices, cybersecurity threats continue to evolve as these risks may now result in devices and control systems being infiltrated. The Guide thus provides timely guidance on how cybersecurity threats should be managed by enterprise users and vendors deploying IoT technology.

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

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

6. South Korea

6.1. COVID-19 and data privacy in Korea

6.1.1. *Introduction*

Korea is recognized as having successfully contained the rapid spread of COVID-19 during the early stages of the outbreak without resorting to the lockdown of specific cities or regions. Even though several factors may have contributed to this success, the minimized isolation/quarantine measures focused on confirmed patients and the transparent disclosure of relevant information have been pointed out as key factors. The strategy behind this approach was to minimize the risk of infection by separating most of the population from minimized risk factors, and this effort seems to have been largely successful. However, since many of these measures were implemented by the Korean government for the first time, their implementation has led to various criticisms and controversies related to privacy infringement. Through a process of trial and error, efforts have been made to achieve a balance between the privacy of individuals and the public interest, and such efforts are still ongoing. Accordingly, we will take a look at the main issues related to the COVID-19 outbreak in Korea from the perspective of data privacy.

6.1.2. *The COVID-19 outbreak and the applicability of Korean data privacy laws*

(a) *Principles*

Article 17 of the Constitution of Korea stipulates that "The privacy of no citizen shall be infringed", and thereby guarantees the privacy of individual citizens against the state. In 2005, the Constitutional Court of Korea took one step further and ruled that the right of "informational self-determination", derived from Article 17, is a fundamental right protected by the Constitution.

Based on such protection granted under the Constitution, the Personal Information Protection Act ("PIPA") exists as Korea's general data privacy law. In addition to the PIPA, there are a number of sector-specific laws such as the Act on Promotion of Information and Communications Network Utilization and Information Protection (which applies to the processing of personal information collected online), the Act on the Protection and Use of Location Information (which applies to the processing of location information), the Credit Information Use and Protection Act (which applies to the processing of credit information), and the Medical Service Act (which applies to the processing of medical data).

Under the PIPA and the abovementioned sector-specific laws, the opt-in consent of data subjects serves as the primary legal basis for the collection and processing of personal information. If consent is not obtained, then personal information may only be collected and processed if such collection/processing is specifically permitted under an applicable law.

(b) *The collection and processing of information under the Infectious Disease Control and Prevention Act ("IDCPA")*

Korea previously went through a very painful experience with the MERS outbreak which took place from May to July 2015. More than 12,000 people were quarantined, 186 were infected and 38 ended up dying. What exacerbated this ordeal back then was the absence of an information disclosure rule. The Korean government appears to have been able to identify more than 10,000 people suspected of having the disease, but there was no legal provision it could rely on at the time to publicly disclose the relevant information – the name of the hospital which became the epicentre of the disease outbreak. However, this decision actually brought about mass panic throughout the country and caused the general population to harbour a fundamental distrust against the Korean government.

In the aftermath of this painful ordeal, the IDCPA was amended to grant broad authority to the Korean government to collect and process the personal information of individuals who test positive for an infectious disease ("Confirmed Patients") and individuals who are suspected of being infected by an infectious disease ("Suspected Patients") without the consent of such individuals. Consequently, the personal information of Confirmed Patients and Suspected Patients connected to the recent COVID-19 outbreak can now be collected, processed and disclosed by relevant Korean authorities pursuant to the IDCPA.

(c) *Information which can be processed under the IDCPA*

Under the IDCPA, relevant Korean authorities may request and collect not only the basic personal details (e.g., name, address, and telephone number) of Confirmed Patients but also various other information such as medical records, immigration records, details of credit card/transportation card usage, CCTV recordings, mobile phone GPS coordinates, etc. This legal authority makes it possible to track and disclose the movement routes of Confirmed Patients and Suspected Patients. However, the actual scope of information that is publicly disclosed is limited to those on Confirmed Patients. Public disclosures of the movement routes of Confirmed Patients are usually made by local government authorities to prevent the risk of further contact with such individuals. A number of apps and web services related to COVID-19 that use such publicly disclosed information have been introduced in the wake of the COVID-19 outbreak and appear to have contributed to containing the spread of the disease.

(d) *Expansion of privacy infringement risk and related criticism*

However, these measures have raised various privacy issues for the individuals whose information is collected and disclosed as above by Korean authorities. The most typical problem is the re-identification risk of pseudonymized information.

When information on the movement routes of Confirmed Patients is disclosed to the public, only pseudonymized information (e.g. "Confirmed Patient No. 6", "Confirmed Patient No. 31") instead of their actual names is revealed. However, there have been reported cases where the identities of Confirmed Patients were compromised after people were able to ascertain their identities by combining publicly disclosed information with other information such as gender, year of birth, area of residence, and route details and thereby infringing the privacy of these individuals. Consequently, criticism against this risk of privacy infringement has been raised continuously.

In response, the National Human Rights Commission of Korea ("NHRC") issued a statement on March 9, 2020, highlighting the fact that there have been serious cases of human rights violations involving the disclosure of more than the minimum necessary amount of personal information of individuals. The NHRC recommended that such disclosures be modified so that only the minimum amount of personal information necessary to achieve the public purpose is disclosed. Thereafter, health authorities have been devoting efforts to refrain from disclosing any information which could lead to identification (e.g. detailed address information, names of employers) unless deemed exceptionally necessary, and it appears that such efforts are still ongoing.

(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 aligned 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 has often been mentioned as one of the main reasons preventing IT service providers 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. However, the idea of transferring Article 25 to the PIPA was discarded during the bill review process after it

was criticised by several legal and industry experts and data handlers/ICSPs.

(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.

6.1.3. *Conclusion*

The current COVID-19 outbreak represents the most seminal case to date (since data privacy laws were first enacted in Korea) where the competing interests of individual privacy and the public's right to know are most clearly at odds with one another and in terms of the number of Korean residents that have been affected (previously, the most notable case involving these competing interests related to the public disclosure of the identity of sex offenders which garnered considerably less interest). As of April 2020, the collection and disclosure of such information has become a national issue as the information on the movement routes of more than 10,000 Confirmed Patients has been publicly disclosed in Korea while the number of Suspected Patients has been estimated to be in the hundreds of thousands.

In a pandemic situation such as the recent COVID-19 outbreak, the compelling public interest to protect the vast majority of the population from the risk of infection and the need to protect the privacy of individual patients who have not committed any crime are both important legal interests that cannot be ignored. Once the current COVID-19 outbreak has subsided, it seems very likely that discussions on the competing interests of individual privacy and the public's right to know will resurface again. It is difficult to predict how such discussions will take shape and what conclusions they may end up bringing. One thing that is certain is that there is a lesson to be learned from this latest ordeal and it is imperative that we actually do.

Kwang Bae Park (Partner), Lee & Ko (kwangbae.park@leeko.com); Sunghee Chae (Partner), Lee & Ko (sunghee.chae@leeko.com); Jaeyoung (Jay) Chang (Associate), Lee & Ko (jaeyoung.chang@leeko.com)

7. Thailand

7.1. *Law on e-meetings*

In 2014, under the Thailand military coup government, the National Council for Peace and Order ("NCPO") effected an update in the law for conducting meetings using electronic technology.

As part of the update, the NCPO published the "Notification No. 74/2557" ("*NCPO Notification*"). The NCPO Notification was applicable to "any meeting which the law requires to be held", including company directors', extraordinary and annual shareholders' meetings. Following the issuing of the NCPO Notification, not only could such meetings be conducted electronically, but they could also be initiated by electronic notice (i.e. e-mail).

The NCPO Notification was followed shortly by the issuance of the "Notification of the Ministry of Information and Communication Technology Re: Standards for Electronic Conferencing Security B.E. 2557" which detailed technical security requirements for implementing the NCPO Notification. Two years later, the Ministry of Commerce, Department of Business Development also published the Clarification re Electronic Meeting No. 13/2559 (2016) ("*DBD Clarification*").

7.1.1. *Restrictions in previous regulations*

Unfortunately, these laws contained certain restrictions which severely limited their utility. In particular, both the NCPO Notification and the DBD Clarification required, inter alia, the following as a prerequisite to any electronic meetings having legal effect:

(a) all meeting participants had to be physically present in Thailand at the time of the meeting; and
(b) at least one-third of the meeting quorum had to be physically located together in one venue.

In addition, these rules required public companies, trade associations and chambers of commerce to amend their by-laws in order for any electronic meetings held to be legally effective.

7.1.2. *Recent proposals*

In light of the recent COVID-19 pandemic, the government has initiated various efforts to reduce the spread of the virus, including a declared state of emergency, imposing travel restrictions and a broad nationwide lockdown. As a result, Thailand's Joint Foreign Chambers of Commerce have recently submitted the following proposals to the Prime Minister's office in relation to the requirements for electronic meetings:

(a) to waive the requirement for physical presence in Thailand, or require physical presence for only a majority of attendees;
(b) to waive the requirement for one-third quorum physical attendance at one venue; and
(c) to waive the requirement for trade associations and chambers of commerce to amend their by-laws before being able to conduct meetings electronically.

Utilizing the centralized powers of the Prime Minister's office under the Emergency Decree on Public Administration in Emergency Situations B.E. 2548 (2005), the Prime Minister has the authority to implement such waivers (either temporarily or permanently) on behalf of the relevant ministries (Ministry of Commerce and Ministry of Digital Economy and Security).

7.1.3. *Latest updates*

On 19 April 2020, the Thai government eventually enacted the Emergency Decree on Meetings via Electronic Media (2020) ("*2020 Decree*"). The 2020 Decree revokes the old law contained in the NCPO Notification.

The new 2020 Decree applies to all meetings required by law and eliminates all the restrictions previously contained in the NCPO Notification, such as: (a) the physical presence of all participants in Thailand; (b) requiring 1/3 of the quorum in a single physical venue; and (c) requiring by-laws to be amended for public companies, trade associations and chambers of commerce.

However, the 2020 Decree maintains the same security requirements in relation to the: (a) recording of sound and/or videos of meetings; and (b) recording of electronic traffic data. It also introduces a new requirement for meetings to permit a method for secret voting as well as open voting.

The 2020 Decree became immediately effective as of 19 April 2020.

John Fotiadis (Director), Atherton Legal, (johnf@athertonlegal.com)

Declaration of Conflict 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.