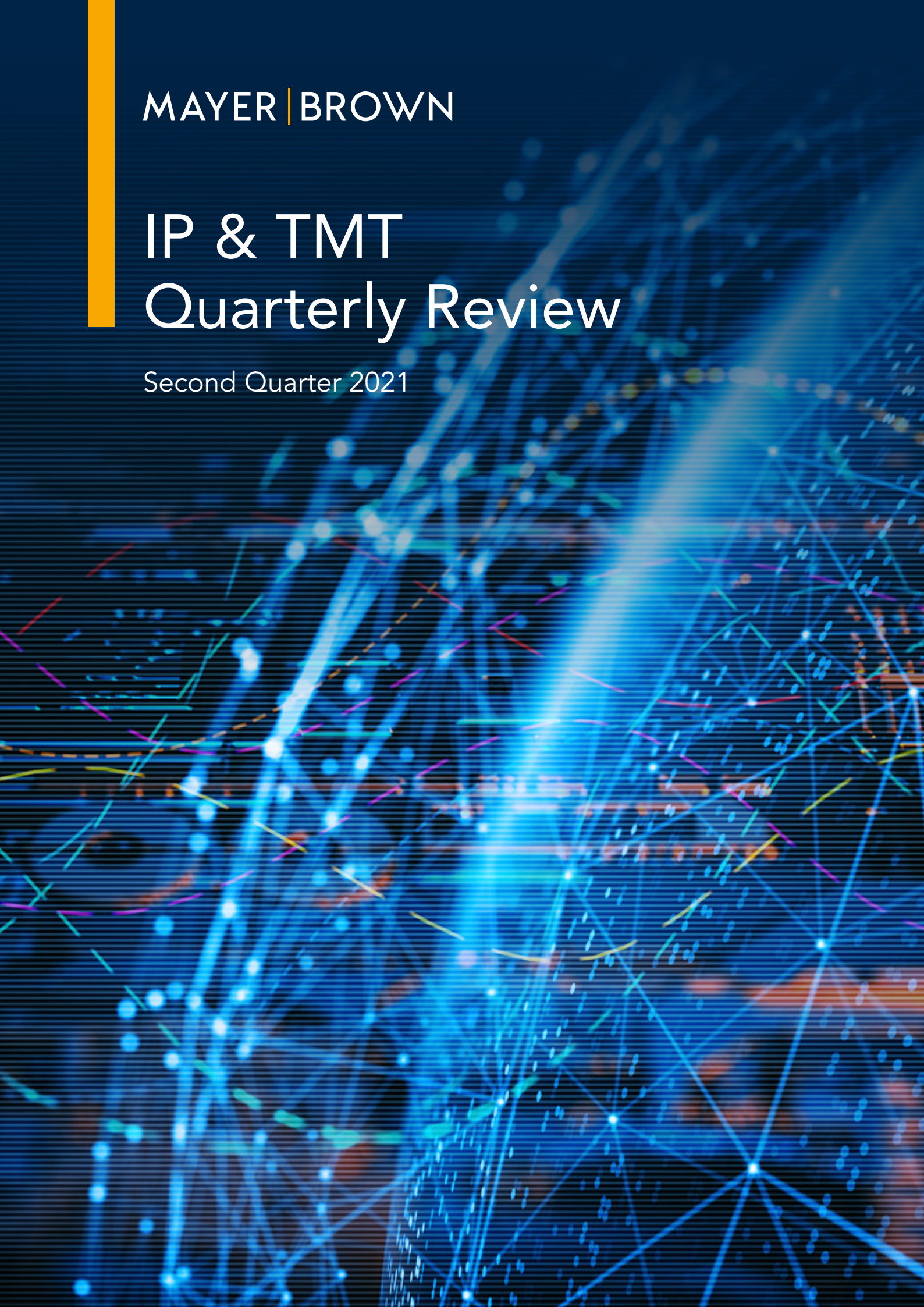
MAYER | BROWN

IP & TMT Quarterly Review

Second Quarter 2021



Contents

Hidden or in Plain View?: China Issues Draft Specification on De-Identification of Personal Information

By **Gabriela Kennedy, Partner**
Mayer Brown, Hong Kong

Karen H.F. Lee, Counsel
Mayer Brown, Hong Kong/Singapore

In May 2021, China released the draft Information Security Technology – Specification for the Classification and Evaluation of the Effect of Personal Information De-identification ("**Draft Specification**"), for public consultation. The Draft Specification proposes the introduction of a new classification system for de-identified personal information, based on the risk of re-identification.

What are the Current Laws Governing Personal Information?

China does not have a single overarching law that regulates the handling of personal information. A piecemeal approach is currently used, with the main provisions found in the Cybersecurity Law ("**CSL**"), the Civil Code[1], telecommunications regulations, consumer rights law, tort law, criminal law and industry specific laws, as well as supplemental interpretations and measures. There are also a number of non-binding

1 Civil Code took effect on 1 January 2021.

measures and guidelines in relation to data protection. Whilst non-binding, compliance with such guidelines is highly recommend and carries significant weight with regulators. This includes the updated Information Security Technology – Personal Information Security Specification 2020 ("**2020 PI Specification**")[2].

In April 2021, the second draft of the new Personal Information Protection Law ("**Draft PIPL**") was released for public consultation. The Draft PIPL is expected to be finalised later this year, and brought into operation at the beginning of 2022. Once passed, it will become China's first comprehensive law that protects personal information, and will work in tandem with the above matrix of existing laws that deal with data protection[3].

Personal Information, Anonymisation and De-Identification

Personal information, as well as de-identified information, will be subject to the restrictions under the CSL, 2020 PI Specification, other related laws, and (once passed) the Draft PIPL. However, anonymised data is expressly excluded from the definition of personal information, and will not be subject to those restrictions (including the cross-border transfer requirements).

De-identified data is often confused with anonymised data. This can present major risks, as whilst anonymised data does not constitute personal information, de-identified data is still considered personal information and is therefore subject to regulation. So what constitutes personal information, anonymised data and de-identified information?

There is currently no single consistent definition of personal information under the laws of China. Under the CSL and Civil Code, personal information means any information that can be used independently or in combination with other information, to identify a natural person. However, the 2020 PI Specification expands the definition of personal information to also include any information that is associated with a natural person's activities. Under the Draft PIPL, personal information is defined even more broadly as any information recorded in any format, which relates to an identified or identifiable individual.

With regard to anonymised data, it is essentially any personal information that has undergone an irreversible process so as to make it impossible to identify or associate it with a specific natural person. In contrast, de-identification is essentially pseudonymised personal information, where it is still possible to identify or associate the information with a natural person when used in combination with other data. Pseudonyms, encryption, hash functions or other technical means are usually used to replace the personal identifiers in personal information in order to convert it to "de-identified" data. For example, using an internal customer reference number to store a customer's records would amount to de-identified data, as the identity can still be discovered when the customer reference number is cross-referenced against other data held by the company.

De-Identification Requirements

As mentioned, de-identified data (but not anonymised data) still constitutes personal information and is subject to the CSL, 2020 PI Specifications and other relevant laws. The 2020 PI Specification includes several requirements relating to de-identification to help protect the personal information from any data breach. For example, it requires data controllers to de-identify personal information immediately after it has been collected, and to take technical and operational measures to separately store the information enabling the re-identification of the relevant natural persons. Whilst non-binding, compliance with the 2020 PI Specification is taken into account by the regulatory and enforcement authorities in the event of an investigation.

To better assist entities with the de-identification process, the Information Security Technology – Guidelines for De-identifying Personal Information

2 Information Security Technology – Personal Information Security Specification GB/T 35273-2020.

3 Please refer to our article 'Full Steam Ahead: Second Draft of China's Personal Information Protection Law and New Data Security Law'

("**Guidelines**")[4] were implemented and provide detailed guidance on how to carry out de-identification.

Draft Specification – What's New?

In furtherance of the Guidelines, the Draft Specification introduces a system for classifying de-identified personal information based on the risk of re-identification. In total, there are 4 levels of identifiability:

1. Level 4 – Aggregated data
2. Level 3 – Data with an acceptable risk of re-identification
3. Level 2 – Data from which direct identifiers have been removed
4. Level 1 – Data from which the data subject is directly identifiable

Personal information that carries the highest risk of re-identification will fall under Level 1, and those that carry the lowest risk will fall under Level 4 (i.e. de-identified personal information that cannot be linked to a particular data subject, such as aggregated data). Once the risk of identifiability is confirmed and the de-identified personal information is classified, companies will be able to better evaluate the effectiveness of their de-identification activities and the security of its data, particularly when data sharing is required.

Akin to the Guidelines, the Draft Specification provides a non-exhaustive lists of common direct and quasi-identifiers. The definitions of these terms remain largely the same: direct identifiers means information that can be used in isolation to identity a person, whereas quasi-identifiers are personal attributes that must be used in conjunction with other information for identification purposes. It is, however, worth noting that compared to the Guidelines, an individual's facial recognition data is added as a direct identifier under the Draft Specification, making it possible to safeguard such data through de-identification.

Conclusion

The Draft Specification is just one in a suite of many data related draft specifications and measures that were issued by the Chinese government in April 2021 – likely fuelled by the release of the second Draft PIPL and second draft Data Security Law. Although the Draft Specification (once passed) will only act as a national standard rather than a binding law, it will help companies assess their de-identification practices to minimise the risks of any data breach. It is important to remember that whilst de-identification is an essential mechanism for protecting personal information – it does not equate to anonymization, and that de-identified data is still subject to data protection laws.

*The authors would like to thank **Sophie Huang**, Intellectual Property Officer at Mayer Brown, for her assistance with this article.*

4 Information Security Technology – Guidelines for De-Identifying Personal Information GB/T 37964-2019 (came into operation 1 March 2020).

China's Social Credit System – How Do You Rate?

By **Gabriela Kennedy, Partner**
Mayer Brown, Hong Kong

Karen H.F. Lee, Counsel
Mayer Brown, Hong Kong/Singapore

The Social Credit Regulation of the Guangdong Province ("**Regulation**"), which was passed recently by the Standing Committee of the Guangdong Provincial People's Congress, came into effect on 1 June 2021. The Regulation seeks to establish rules for the province's social credit system and introduces restrictions on the collection of biometric information from individuals. The Regulation is just one amongst many regulations concerning the social credit system which have been issued over the last five years. In the past year alone, a number of regulations have been issued to deal with the impact of the Covid 19 pandemic on the social credit system. These regulations apply to companies that make a decisive contribution to the fight against Covid-19, making them eligible to receive certain benefits, and also seek to keep in check the exploitation of the pandemic or breach of quarantine and other Covid-19 restrictions.

Background

Since the formal launch in 2014 of the social credit system, China has been fine tuning this system through which the trustworthiness of individuals, companies and government entities can be monitored and assessed based on their assigned credit ratings. It essentially acts as a tool to track compliance with China's laws and regulations.

Whilst data aggregation is centralised, the system itself is not unified, and there is no consistent definition of "social credit" or the method in which a credit score is determined. Instead, the system is made up of a vast number of national and provincial policies and regulations issued by various authorities. Foreign companies with a presence in China (e.g. legal person or branch office) are also subject to China's social credit system and the myriad of related regulations.

Blacklists are used to name and shame and penalise individuals or entities that breach laws and regulations, and red lists are used to reward those who have been consistently compliant. For individuals, being on a blacklist could potentially restrict their ability to travel, their employment prospects and their access to financial services. Different blacklists are managed by various government and regulatory authorities across China.

The Regulation

Under the Regulation, social credit information is defined as objective data and materials used for the purpose of identifying, analysing and determining a subject's social credit status. Such information includes public credit information (i.e. information generated and acquired by the state organs and organizations that manage public affairs, during the course of them carrying out their duties and providing public services) and market credit information (i.e. information created and obtained by market credit service establishments, credit service industry organizations and other enterprises and social organisations when engaging in production, business and social service activities).

Unless the credit subject has given his or her consent or it is permitted under law, an individual's name, date of birth, ID number, address and telephone number, which are collected as part of their public credit information, must not be disclosed. If disclosure is necessary, then safety measures should be taken beforehand to protect the data. Consent is also required when the collection of market credit information involves the credit subject's personal information, and the credit subject must be informed of the types of personal information being collected, the collection method, possible use of the information, and their rights and obligations. Collection of an individual's biometric data, such as blood type, medical history and fingerprint data, is prohibited.

Following Tianjin and Dalian, Guangdong is now one of the first few pioneers to ban biometric data collection in social credit ratings.

Takeaways

The social credit system is still a key aspect of China's five year plan (2021 to 2025) for the construction of a rule of law society. China will likely work towards introducing a more unified and cohesive social credit system over the next few years. Data privacy concerns are likely to be a key factor, as negative social credit scores can have a serious impact on an individual's rights. The ability for individuals and companies to repair their credit score, and how data will be used and shared (publicly and amongst different organisations and government authorities), particularly in relation to blacklists, will also be a key focus.

*The authors would like to thank **Sophie Huang**, Intellectual Property Officer at Mayer Brown, for her assistance with this article.*

Full Steam Ahead: Second Draft of China's Personal Information Protection Law and the New Data Security Law

By **Gabriela Kennedy, Partner**
Mayer Brown, Hong Kong

Karen H.F. Lee, Counsel
Mayer Brown, Hong Kong/Singapore

On 29 April 2021, the second drafts of China's Personal Information Protection Law (Second Draft PIPL)[5] and the Data Security Law (DSL) were released. Once passed, the Second Draft PIPL will become China's first comprehensive law that protects personal information. On 10 June 2021, the Standing Committee of the National People's Congress passed the DSL, which will come into force on 1 September 2021. The DSL will further regulate data processing activities that could impact national security, particularly "important data".

While the Second Draft PIPL and the final DSL do not substantially depart from their earlier drafts, some further obligations and clarifications have been added. We summarise some of these key changes below.

5 See our article regarding the first draft of the PIPL: https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2020/12/asi_ip_tmt_quarterlyreview_2020q4.pdf

Second Draft PIPL

DATA PROCESSORS

In a major departure from the previous draft, the Second Draft PIPL expands the obligations imposed on third parties entrusted to handle personal information (i.e., the equivalent of a data processor under the GDPR (the EU General Data Protection Regulation)).

Under the first draft, data processors were not directly regulated. Instead, they were only required to process the personal information in accordance with the relevant data processing agreement with the data controller (referred to as the "personal information processor" under the Second Draft PIPL), to delete or return the personal information once the agreement is fulfilled or terminated and to not further sub-contract the processing of the personal information, unless it obtains the data controller's consent.

Under the new Article 58, data processors must perform the relevant obligations under Chapter V of the Second Draft PIPL and adopt necessary measures to ensure the personal information is kept secure. In particular, this may mean that overseas data processors that process personal information to provide goods or services or analyse or assess the behaviour of data subjects in China (or under any other circumstances prescribed under the laws or regulations), will need to appoint a local representative or establish an office in China[6]. This may have major implications for foreign companies that have no onshore operations, but which are providing services to data controllers handling personal information collected in China.

In addition to establishing a local presence, data processors will also now need (among other things) to conduct regular audits to verify that their processing activities are compliant with China's laws and regulations; carry our risk assessments prior to processing sensitive personal information, using automated decision-making, disclosing any personal information or making any cross-border transfers; comply with breach notification obligations; and comply with the new obligations imposed on large internet platform service providers (discussed below).

OBLIGATIONS ON LARGE INTERNET PLATFORM SERVICE PROVIDERS

Another significant amendment proposed by the Second Draft PIPL are the additional obligations on data controllers which provide basic online platform services to a substantial number of users and which operate complex business models[7]. Such data controllers would be required to:

1. Establish an independent body, mainly consisting of external personnel, to oversee the data controller's processing activities;
2. Stop providing services to those who are offering products or services via the data controller's online platform, who are in serious violation of the data processing requirements under the relevant laws and regulations; and
3. Regularly publish corporate social responsibility reports in relation to personal information protection.

It is likely that further measures or interpretations will be issued to provide clarity on the application of the above requirements. In particular, clarification will be welcomed in respect of what would constitute a substantial number of users or complex business models, what would amount to a serious violation of the laws and regulations, and what needs to be included in the social responsibility reports.

It is important to remember that as with the original draft, the Second Draft PIPL is intended to have extra-territorial effect. Article 3 provides that the Second Draft PIPL shall apply to any processing of personal information that occurs outside China, if the purpose of processing is to provide products or services to individuals in China, to analyse and evaluate the behaviour of individuals in China, or any other circumstances specified by the laws or regulations. The effect of this article is that online platform service providers based overseas, may need to comply with the above requirements even if they do not have an onshore presence, and/or will have to establish an office or appoint a legal representative in China[8].

6 Article 53 and 58 of the Second Draft PIPL.
7 Pursuant to Article 58 of the Second Draft PIPL, these obligations may also apply to data processors.
8 Article 53 and 58 of the Second Draft PIPL.

LEGAL BASIS FOR PROCESSING AND CONSENT

The processing of personal information that is publicly available has been added as a new legal basis for processing under the Second Draft PIPL. This departs from the GDPR, which does not include publicly available personal information as a legal basis for processing. Under the Second Draft PIPL, personal information processors (the equivalent of data controllers under the GDPR) can process personal information if one of the following legal bases applies[9]:

1. The data subject has provided their consent;
2. The processing is necessary for the performance of a contract to which the data subject is a party;
3. The processing is necessary for the fulfilment of duties or obligations imposed under laws or regulations;
4. There is a need to respond to public health emergencies or to protect an individual's life, health or property in an emergency situation;
5. The personal information is already publicly available, and the processing is within a reasonable scope in compliance with the PIPL;
6. The personal information is being processed for the purposes of conducting news reporting, supervising public opinion or other such activities that are in the public interest and the processing is within reasonable scope; and
7. The processing is permitted pursuant to other laws and regulations.

Article 13 of the Second Draft PIPL makes it clear that obtaining the data subject's consent is not mandatory if the processing falls within the scope of any other legal basis set out under paragraph (2) to (7) above. Based on the wording of Article 30 of the Second Draft PIPL, it seems that this equally applies to the collection of sensitive personal information, where the express consent of the data subject will only be needed if the personal information processor is seeking to rely on consent as the basis for processing, unless other laws or regulations stipulate that written consent is required[10]. In contrast, Article 39 of the Second Draft PIPL does not expressly limit the requirement for express consent on the cross-border transfer of personal information to only situations where consent is being relied on as the basis for processing. This conflicts with Article 13. Further clarity may be needed on whether express consent may still be required for cross-border transfers, even if other grounds for processing apply.

CROSS-BORDER TRANSFERS

The cross-border transfer requirements under the Second Draft PIPL, remain largely the same as in the original draft. The only key change is that if personal information is being transferred on the basis of an agreement with the foreign recipient, such agreement must be based on the "standard contract" stipulated by the Cyberspace Administration of China (CAC).

As a brief recap, the Second Draft PIPL now provides that personal information cannot be transferred outside of China, unless one of the following conditions are met[11]:

1. A security certification is obtained, which is conducted by an accredited body in accordance with regulations specified by the CAC;
2. An agreement with the foreign recipient is entered into based on the "standard contract" stipulated by the CAC, which sets out each party's respective rights and obligations, and ensures that the personal information will be protected to the same standard as that provided under the Draft PIPL; or
3. The transfer is in accordance with other laws or regulations or other conditions prescribed by the CAC.

However, critical information infrastructure (CII) operators and any personal information processors who process personal information at a volume that exceeds the threshold specified by the CAC (still to be determined), can only transfer the personal information overseas if a security assessment is completed by the CAC[12].

Aside from the above, a prior risk assessment must also be conducted by the personal information

9 Article 13 of the Second Draft PIPL.
10 Article 13 and 30 of the Second Draft PIPL.
11 Article 38 of the Second Draft PIPL.
12 Article 40 of the Second Draft PIPL.

processor in relation to the cross-border transfers[13]. Records of the risk assessment must be retained for at least three years.

The above requirements under the Second Draft PIPL are largely consistent with China's Cybersecurity Law (CSL) and draft Measures on Security Assessment of the Cross-Border Transfer of Personal Information issued in 2019 (Draft Measures). Note that separate to the Second Draft PIPL, CII operators and networks operators (essentially any entity that owns or operates a computer network, server or website in China) will need to comply with the data localisation and cross-border transfer restrictions currently in force under the CSL. The Draft Measures have not yet been brought into operation, and are likely to be subject to further amendments to align them with the Second Draft PIPL.

Consistent with the DSL, there are also restrictions under the Second Draft PIPL on the transfer of personal information requested by foreign judicial or law enforcement authorities, unless approval has been obtained from the relevant Chinese authority or it is in accordance with relevant international treaties[14]. The Chinese authorities can also take steps against foreign organisations that engage in processing activities that are seen as harming the rights and interests of Chinese citizens or which endanger national security or public interest (e.g., prohibiting the provision of personal information to them)[15]. Further, if any country adopts what the Chinese authorities deem to be discriminatory measures against China in relation to personal information protection, it may implement reciprocal measures against them[16].

OTHER CHANGES

Some of the other changes introduced in the Second Draft PIPL include the following:

1. A prohibition on the processing of personal information through the use of coercion[17];
2. A requirement to process personal information in a manner that has the least impact on the individual's rights and interests[18];
3. A requirement that personal information processors should make sure that the personal information collected is of high quality and should avoid causing harm to the data subject's rights and interests due to any inaccuracy and incompleteness in the personal information[19];
4. An obligation to obtain the consent of a minor's parents or guardian when data of a person under 14 years of age are collected (under the original draft, this requirement only applied if the personal information processor knew or ought to have known that the personal information concerned a minor)[20];
5. A clarification of the fact that any withdrawal of a data subject's consent to the processing of their personal information will not affect the processing activities that have been carried out before the consent was withdrawn[21];
6. An expansion of the scope of protection of personal information granted under the Second Draft PIPL to apply to deceased individuals, whose rights granted under the law can be exercised by his or her next of kin[22];
7. A requirement for personal information processors to follow principles of openness and transparency, and make known to the public their specific rules for processing, as well as the purpose, method and scope of the processing (this is on top of the notification obligations, which already appear in the first draft)[23];
8. A requirement to provide an opt-out for marketing activities (where personal information is used for commercial marketing purposes and push notifications through automated decision-making)[24]; and

13 Article 55 of the Second Draft PIPL.
14 Article 41 of the Second Draft PIPL.
15 Article 42 of the Second Draft PIPL.
16 Article 43 of the Second Draft PIPL.
17 Article 5 of the Second Draft PIPL.
18 Article 6 of the Second Draft PIPL.
19 Article 8 of the Second Draft PIPL.
20 Article 15 of the Second Draft PIPL.
21 Article 16 of the Second Draft PIPL.
22 Article 49 of the Second Draft PIPL.
23 Article 7 of the Second Draft PIPL.
24 Article 25 of the Second Draft PIPL.

9. Heightened liability for data controllers in situations where an individual claims that their personal information rights have been infringed, the burden of proof now rests with the data controller[25]. The data controller will be liable for damages, unless it can prove that it was not at fault.

DSL

SCOPE OF APPLICATION

The DSL applies to the processing of "data", i.e., any record of information in electronic or non-electronic form, but does not apply to the processing of personal information, state secrets or military data.[26] The final version of the DSL also makes it clear that the law applies to "data processing activities" carried out within the territory of China, replacing the phrase "data activities" used in the first draft. The definition of "data processing activities" is, however, similar to that of "data activities", which includes the collection, storage, use, refining, transmission, provision and disclosure of data. As with the first draft, the final version of the DSL is intended to have extra-territorial effect.

DATA CLASSIFICATION

Under the DSL, the government is tasked with establishing a data classification management and protection system to govern data based on how important or essential the data are to national security and the public interest, and the level of impact that any data leak, tampering, damage or illegal acquisition may have on national security, the public interest or the lawful rights and interests of citizens or organisations. Each sector and region must also establish catalogues to identify important data in the relevant industry, in accordance with the data categorisation and classification systems established by the government, and impose special measures to protect such data. In addition, the final version of the DSL introduces a new category known as "national core data", which includes data relating to China's national security, lifeline of the national economy, people's livelihoods and major public interests, and requires more stringent requirements to be imposed to protect such data.

DATA SECURITY OBLIGATIONS

The final version of the DSL effectively expands the scope of some of the obligations imposed on network operators and CII operators under the CSL. Under Article 27 of the DSL, any entity that carries out data processing activities (which essentially means any entity whatsoever), must establish a data security management system, carry out data security training, and implement technical security and safeguarding measures. For any entities that carry out data processing activities through the internet or other information network, the foregoing data security obligations must be established pursuant to the multi-level protection scheme (MLPS). In addition, where important data is being processed by an entity, it must also designate a data security officer and establish a management office to ensure compliance with its data security obligations.

The MLPS is established by the government and prescribes security measures that must be met depending on different risk classification levels. The higher the risk to national security, social order or economic interests that may occur if an entity's system is damaged or subject to an attack, the higher their classification and the more stringent the security requirements.

CROSS-BORDER TRANSFER OF IMPORTANT DATA BY NON-CII OPERATORS REGULATED

The DSL distinguishes between CII and non-CII operators on the cross-border transfer of important data. CII operators are regulated under the CSL and are broadly defined as entities whose business has the potential to cause harm to national security, national economy, people's livelihood and public interests in the event they suffer a security breach that leads to any destruction or loss of function or data. While CII operators must follow the rules set out under the CSL, the DSL requires non-CII operators to conform to the requirements formulated by the CAC or other government agencies for the overseas transfer of important data[27]. These requirements have not yet been stipulated, and will likely be published over the next year or so.

25 Article 68 of the Second Draft PIPL.
26 Article 3, 51 and 52 of the Second Draft DSL.
27 Article 31 of the DSL.

It is important to remember that CII operators and network operators are also still subject to the CSL, and the requirements relating to data localisation and cross-border transfers.

PENALTIES

Under the original draft, if a foreign judicial or law enforcement authority requested access to data stored in China, such data could not be provided unless approval had been obtained from the competent government authority, or a relevant international treaty applied[28]. Under the final version of the DSL those in breach may now face severe punishments for non-compliance, which include the issuance of rectification orders, suspension of business, revocation of business licences, warnings, and a fine of up to RMB 5 million[29] on the organisation and up to RMB 500,000 on the person in charge and other directly responsible personnel. This places multinational companies in a difficult lose-lose situation, where compliance with a foreign authority's data access request may render them in breach of Chinese law, and non-compliance will render them in violation of the relevant foreign laws or court orders.

The penalties imposed for violating some of the other obligations under the final version of the DSL have also been increased (e.g., raising the fine up to RMB 10 million for serious violations of the cross-border transfer restrictions), and liability has been extended to cover not only those in charge, but also any personnel that was directly responsible for the breach.

Takeaways

Large platform service providers and data processors (even those without operations in China), may be subject to enhanced obligations under the Second Draft PIPL, while any organisation that handles data (even data not seen as "important data") must comply with cross-border transfer restrictions, carry out an MLPS assessment and implement corresponding security measures under the DSL. Both the Second Draft PIPL and the DSL are intended to have extra-territorial effect, and entities that have customers, clients or service providers in China need to pay particular attention to see whether or not they would be caught by these laws once enacted.

Furthermore, the passing of the Second Draft PIPL and the DSL will not over-ride the complex matrix of laws in China relating to data. Companies must still also ensure compliance with the CSL, China's Encryption Law[30], Anti-espionage Security Prevention Work Regulation[31], and other various specific measures and standards (such as those concerning mobile apps and facial recognition technology).

The DSL was passed on 10 June 2021, and will be brought into operation on 1 September 2021. As with many Chinese laws, additional measures and guidelines are likely to be issued by the government in order to provide clarification on the implementation of the DSL.

The Second Draft PIPL is expected to be passed later this year, with possibly some further amendments, and brought into operation at the beginning of 2022. Companies should start reviewing their operations to ensure compliance with the DSL, and keep a sharp eye on further developments in preparation for what is to come.

*The authors would like to thank **Sophie Huang**, Intellectual Property Officer at Mayer Brown, for her assistance with this article.*

28 Article 36 of the DSL.
29 Article 48 of the DSL.
30 Issued on 26 October 2019, and brought into force on 1 January 2020.
31 Issued and brought into force on 26 April 2021.

Dealing with Doxxing: Proposed Amendments to the Hong Kong Privacy Law

By **Gabriela Kennedy, Partner**
Mayer Brown, Hong Kong

Karen H.F. Lee, Counsel
Mayer Brown, Hong Kong/Singapore

On 17 May 2021, the Hong Kong Legislative Council Panel on Constitutional Affairs issued a discussion paper ("**Discussion Paper**") on the proposed amendments to the Hong Kong Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**") to tackle the problem of doxxing.

Background

On 13 January 2020, the Constitutional and Mainland Affairs Bureau had published a paper proposing 6 amendments to the PDPO (including introducing a mandatory data breach notification mechanism and the direct regulation of data processors)[32]. However, the Discussion Paper focused solely on the issue of doxxing.

Doxxing has become a widespread problem in Hong Kong over the last couple of years, and has been a major concern for law enforcement authorities and the Privacy Commissioner for Personal Data ("**PCPD**"). Doxxing involves the publishing of private or personal information online without the

32 See our article 'Out with the Old, In with the New: Proposal for Review of Personal Data (Privacy) Ordinance': https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2020/03/asia_ip_tmt_quarterly_review_2020q1.pdf

relevant individual's consent, usually for harassment or other malicious purposes. Between June 2019 and April 2021, the PCPD handled 5,700 complaints concerning doxxing, and issued 297 requests to 18 websites, social media platforms and forums to remove over 5,905 links – about 70% of which were complied with.

Under the PDPO, the PCPD has limited powers to tackle doxxing activities. Even though the PCPD can refer potential criminal cases to the police and department of justice for investigation and prosecution, the PCPD does not have the power to issue administrative fines or penalties, and cannot order operators of websites, social media platforms or forums to takedown any content that violates the PDPO (any takedowns would be on a voluntary basis). There is also currently no direct offence for doxxing. Instead, prosecutors have tried to rely on other criminal offences to prosecute doxxers, including section 64(2) of the PDPO.

Under section 64(2) of the PDPO, a person commits an offence if they disclose the personal data of an individual obtained from a *data user*, without the *data user*'s consent, which causes psychological harm to the individual regardless of intent. A data user is anyone who controls the collection, holding, processing or use of personal data, which could include the data subject themselves. A person convicted under section 64(2) of the PDPO is subject to a fine of HK$ 1,000,000 and 5 years imprisonment. To date, only 2 people have been convicted under section 64(2) for doxxing[33].

Section 64(2) of the PDPO was never intended to address doxxing, and its limits when it came to proscuting doxxers have become apparent. Most doxxing cases involve the online dissemination of personal data that is repeatedly shared and reposted. This makes it difficult for the PCPD to trace the source of the content, to identify the original data user and determine whether or not it had been disseminated "without the data user's consent".

Amendments

The Discussion Paper proposes 3 key amendments to the PDPO in order to specifically combat doxxing.

(1) THE INTRODUCTION OF A NEW OFFENCE TO DEAL WITH DOXXING

A new offence would be introduced under section 64 of the PDPO, under which a person would commit an offence if they disclose any personal data of a data subject without that data subject's consent, if they do so:

a. with an intent to threaten, intimidate or harass the data subject or any immediate family member, or are reckless as to whether the data subject or any immediate family member would be threatened, intimidated or harassed; or

b. with an intent to cause psychological harm to the data subject or an immediate family member, or being reckless as to whether psychological harm would be caused to the data subject or any immediate family member,

and the disclosure does cause psychological harm to the data subject or an immediate family member. Anyone found guilty of this new offence could face a fine of HK$ 1,000,000 and 5 years imprisonment (for conviction on indictment) or a fine of HK$ 100,000 and 2 years imprisonment (for summary conviction).

(2) THE PCPD TO HAVE THE POWER TO CARRY OUT CRIMINAL INVESTIGATIONS AND PROSECUTION

As mentioned, the PCPD currently has to refer any potential criminal cases to the police or the Department of Justice for investigation and prosecution. The Discussion Paper proposes granting the PCPD the power to carry out her own criminal investigations and initiate prosecutions under section 64 of the PDPO (including the new doxxing offence), in order to help expedite the investigation and prosecution of doxxing offences. Such powers would include:

c. the ability to request relevant information, documents or items from anyone, or require anyone to answer relevant questions to assist with any investigation, where the PCPD has reasonable grounds to believe that an offence has been (or is being) committed under section 64 of the PDPO;

d. the ability to apply to the court for permission to enter any premises, and to seize documents

33 See our article 'Privacy in Politics and the Politics of Privacy': https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2020/12/asi_ip_tmt_quarterlyreview_2020q4.pdf

or items at the premises, on the basis that the PCPD has reasonable grounds: (i) to believe that there has been a contravention of section 64 of the PDPO; and (ii) to suspect that there are documents and things at the premises that can be collected as evidence;

e. the ability to prosecute under the PCPD's own name cases involving contraventions of section 64 of the PDPO or failure to comply with the PCPD's above requests in relation to a criminal investigation; and

f. the ability to apply to the court for an injunction if the PCPD is satisfied that there is or it is very likely that there is a large scale or repeated contravention of section 64 of the PDPO in the society. The intent is to prevent the recurrence of doxxing incidents targeting specific persons or groups (e.g. police officers or government officials).

(3) THE PCPD TO HAVE THE POWER TO ISSUE RECTIFICATION NOTICES

Currently, the PCPD does not have the power to order the removal of any doxxing content. Any non-compliance with a request sent by the PCPD does not amount to an offence, and removal is on a voluntary basis.

Since the removal of the doxxing content is a key to stopping the continued spread of the content and harm to the data subjects concerned, the Discussion Paper proposes that the PCPD be empowered to serve a rectification notice to any person, in order for such person to take rectification actions within a designated timeframe, if the PCPD has reasonable grounds to believe that a contravention of section 64 of the PDPO has been (or is being) committed. The intention is for such power to have extra-territorial effect, so that the PCPD can issue a rectification notice against any person, including any company or platform operator located overseas, which provide services in Hong Kong or to residents in Hong Kong.

The rectification notice must set out the doxxing content, the rectification steps that need to be taken, and the deadline for compliance. Failure to comply with a rectification notice amounts to an offence, unless the recipient can show that they had a reasonable excuse for failing to comply in a timely manner. Under the current proposal, failure to comply with a rectification notice will incur the same penalties as failure to comply with an enforcement notice. Therefore, a first conviction will attract a fine of up to HK$ 50,000 and 2 years imprisonment (with a daily fine of HK$ 1,000 if the offence continues), and any subsequent convictions will attract a fine of up to HK$100,000 and 2 years imprisonment (with a daily fine of HK$ 2,000 if the offence continues). However, enforcing such penalties against foreign companies with no presence in Hong Kong may be difficult.

It is also proposed that any person can submit an appeal to the Administrative Appeals Board to challenge a rectification notice within 14 days of receiving it. However, they would still be obligated to comply with the rectification notice within the stipulated timeframe pending the issuance of the Administrative Appeals Board's final decision.

Final Thoughts

The current wording of the new offence of doxxing is broad enough that it may have the result of being used to prosecute other behaviour, such as cyber bullying, voyeurism "revenge porn" or the distribution of other intimate material. It will be interesting to see how the proposed new offence under the PDPO will be interpreted when the new offences being separately proposed against voyeurism, intimate prying, non-consensual photography of intimate parts, and the distribution of related images[34] are also brought in.

The amendment bill is expected to be issued by the end of 2021. In the meantime, it is likely that additional papers will be issued concerning the other key amendments to the PDPO proposed by the Constitutional and Mainland Affairs Bureau.

34 "Proposed Introduction of Offences of Voyeurism, Intimate Prying, Non-consensual Photography of Intimate Parts, and Related Offences" issued on 8 July 2020 by the Hong Kong Security Bureau. See are article entitled 'Peek-a-Boo I've Caught You – New Offences Against Upskirt Photos and Blackmail': https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2020/09/asi_ip_tmt_quarterlyreview_2020q3.pdf

Open the Floodgates: First Award of Compensation for Injury to Feelings under Hong Kong Privacy Law

By **Gabriela Kennedy, Partner**
Mayer Brown, Hong Kong

Karen H.F. Lee, Counsel
Mayer Brown, Hong Kong/Singapore

On 19 February 2021, the District Court of Hong Kong issued the first ever award of compensation for injury to feelings under section 66 of the Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**")[35].

Background

Under section 66 of the PDPO, an individual is entitled to compensation if they suffer any damage, including injury to feelings, as a result of a breach of the PDPO by a data user, and the breach concerns the individual's personal data.

The facts of this case can be summarised as follows:

- The Defendants (a married couple) sent a letter to the Principal and English Panel Chairperson of the primary school at which the Plaintiff is employed ("**Letter**").
- The Plaintiff is the niece of one of the Defendants, and lives in the same area as them.

35 Tsang Po Mann v. Tsang Ka Kit [2021] 1 HKLRD 1301

- The Letter contained allegations that the Plaintiff treated herself as an English person and often used English to argue with her neighbours, that she opened doors to other people's houses without their authority, and that she owned a dog and let it foul the pavement and other public places and did not clean up after it.
- The Letter also included four photographs, which were still images captured from CCTV cameras installed at the Defendants' home. The photographs showed the Plaintiff standing in front of the Defendants' building or on a road, either alone, with her dog or with other people.

The Plaintiff issued proceedings against the Defendant for defamation and injury to feelings under section 66 of the PDPO. Whilst the Plaintiff was not successful in her defamation action, the District Court found that she was entitled to HK$ 70,000 in compensation for injury to feelings under the PDPO.

The Decision

The CCTV cameras had been installed at the Defendants' home for security purposes, and they were held to be joint data users for the purpose of the PDPO (i.e. a person who alone or jointly with others, controls the collection, holding, processing or use of the personal data). Under Data Protection Principle 3(1) ("**DPP 3**") of the PDPO, data users must not, without the prescribed consent of the data subject, use the data collected for a new purpose. The District Court found that the use of the CCTV images attached to the Letter by the Defendants amounted to a new purpose of use, and failure to obtain the consent of the Plaintiff was a breach of DPP 3.

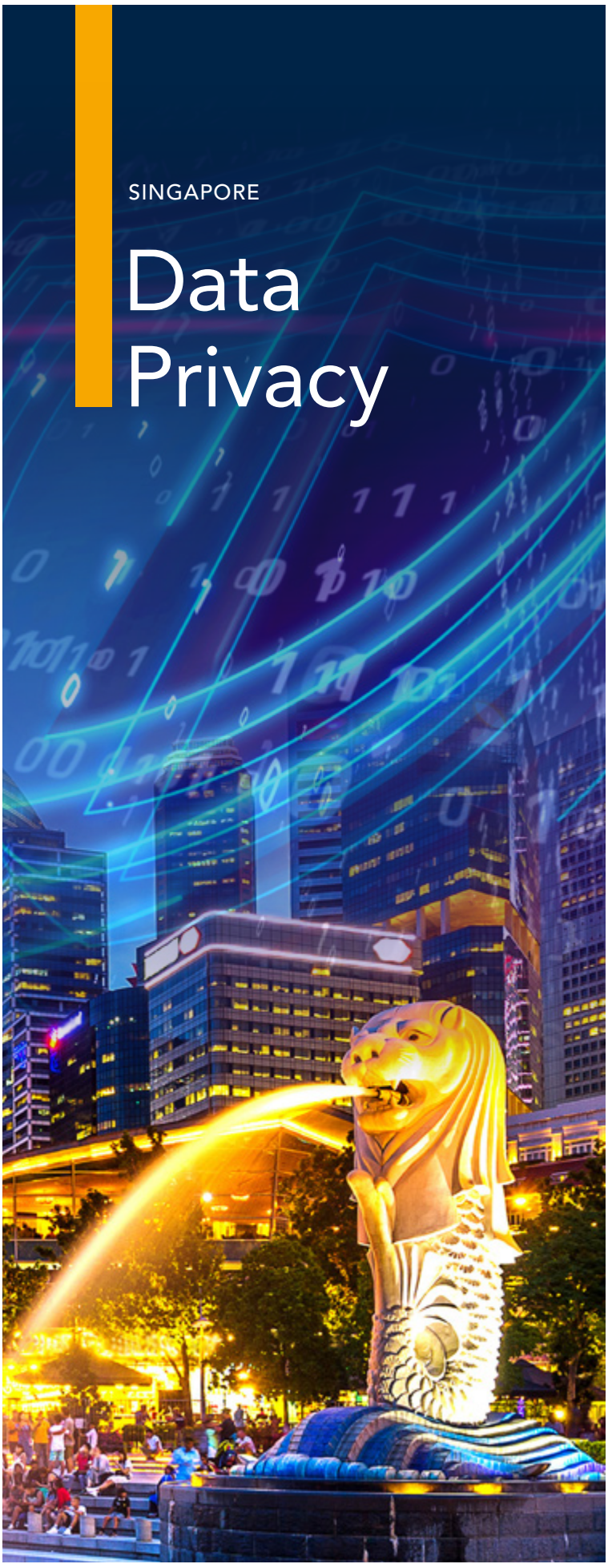
At the time of collection, CCTV footage might not be considered to amount to a collection of personal data, as the data user was not seeking to identify any individual by capturing CCTV footage, unless and until a security breach occurred. However, in this case, the Defendants were clearly seeking to identify the Plaintiff when they selected still images of her from the CCTV footage, in order to send them along with the Letter to the Plaintiff's employer. Some of the CCTV cameras even covered the building where the Plaintiff resides, and the Plaintiff could not have expected (or ever agreed) that the Defendants would use the CCTV footage in such a manner.

The Plaintiff claimed that after she found out about the Letter she had been unable to sleep, suffered from paranoia and fear that she was being watched and filmed at all times. She had to seek medical assistance and was prescribed sleeping pills. Whilst the CCTV images themselves were not seen as particularly offensive, the District Court found that there was a real threat that the Defendants could misuse the CCTV footage against her.

Since this is the first case of compensation being awarded for injury to feelings under the PDPO, in assessing the level of damages payable, the District Court referred to discrimination cases concerning injury to feelings as a precedent. It awarded compensation in the amount of HK$ 70,000, taking into account the manner in which her personal data was misused and the serious nature of the injury to her feelings.

Takeaways

This case may open the floodgates to further claims being issued against data users for injury to feelings, especially in relation to doxxing cases that have received increased attention over the last year. For example, victims of doxxing may seek compensation against the individuals or platforms that have published their personal data for the purposes of inciting harassment. With the current climate in Hong Kong and the proposed changes to the PDPO to tackle doxxing, courts may be more than willing to grant compensation for injury to feelings in such circumstances.



Singapore Releases Updated Guides on Managing Data Breaches and Active Enforcement

By **Karen H.F. Lee, Counsel**
Mayer Brown, Hong Kong/Singapore

Cheng Hau Yeo, Associate
Mayer Brown, Singapore

On 15 March 2021, the Singapore Personal Data Protection Commission ("**PDPC**") issued updated versions of the "Guide on Managing and Notifying Data Breaches under the PDPA" ("**Data Breach Guide**") (formerly known as the Guide to Managing Data Breaches 2.0) and the "Guide on Active Enforcement" ("**Enforcement Guide**"). The latest updates to the Data Breach Guide and Enforcement Guide serve to provide additional clarification and guidance to organisations in light of the recent amendments to Singapore's Personal Data Protection Act 2012 ("**PDPA**").

Data Breach Guide

The Data Breach Guide contains three key parts: (i) Part I sets out recommended good practices for organisations to adopt so as to be able to better identify and prepare for data breaches; (ii) Part II sets out certain important factors for organisations to take into consideration when responding to data breaches; and (iii) Part III provides details of the mandatory data breach notification obligation ("**DBN Obligation**"), which was recently introduced as part of the latest amendments to the PDPA.

PART I – PREPARING FOR A DATA BREACH

The Data Breach Guide clarifies that a data breach can result from a variety of different circumstances and provides a non-exhaustive list of these possible causes (e.g. malicious activities, human error, computer system weaknesses, etc.), which may be helpful in aiding organisations in identifying a data breach.

Organisations are advised to implement appropriate measures which will enable them to properly monitor and take any pre-emptive actions where necessary to prepare for a data breach. Such monitoring should be carried out through regular management oversight as well as using technical tools (e.g. traffic monitoring tools, real-time intrusion detection software, security cameras, etc.). Monitoring measures may include conducting regular reviews of system and application logs, and subscribing to relevant information sources for security alerts.

It is also highly recommended for organisations to establish a data breach management plan to help their employees manage and respond to data breaches more effectively. In particular, an effective data breach management plan should include: (i) a clear definition of a suspected and confirmed data breach; (ii) steps to take for reporting a data breach within the organisation; (iii) strategies for containing, assessing and managing a data breach; and (iv) composition and responsibilities of the data breach management team. In our experience, having a data breach management plan is not enough – it is vital that organisations provide regular training to their employees through table top simulations, so that they know how to implement the plan in practice, if a data breach ever occurs.

PART II – RESPONDING TO A DATA BREACH

The Data Breach Guide sets out four main steps (C.A.R.E) to be taken in the event of a data breach:

i. **Contain** the incident to prevent further breach of data and carry out steps to mitigate the potential impact resulting from the breach. Upon becoming aware of a data breach, the organisation should conduct an initial appraisal to determine the severity of the breach. With such information, the organisation may then identify the appropriate containment actions to be taken and also consider alerting law enforcement and other regulatory authorities (if it suspects that any criminal activities are involved or if required by sector-specific requirements);

ii. **Assess** the data breach to ascertain the root cause and effectiveness of containment measures that have been carried out and, where necessary, make continuing efforts to avoid any further impact of the data breach. Once the breach has been contained, the organisation should carry out a detailed assessment of the breach, whether its containment measures have been successful, and the effectiveness of any technological protection applied to the affected personal data;

iii. **Report** the data breach to: (a) the PDPC (either on a mandatory basis if the DBN Obligation applies or on a voluntarily basis if the DBN Obligation is not applicable); and/or (b) the affected individuals (if required under the DBN Obligation). For data breaches that will likely garner widespread public attention or interest, or if the organisation wishes to seek guidance from the PDPC on providing notification to the affected individuals, the organisation is strongly recommended to notify and seek advice from the PDPC before proceeding to notify the affected individuals;

iv. **Evaluate** the organisation's response to the data breach and the measure(s) that may be carried out to prevent any future data breaches. Such measures may include carrying out a root cause analysis of the breach, conducting a review of the organisation's existing policies and procedures, and assessing the data intermediaries involved in the data breach.

PART III – THE DBN OBLIGATION

This Part provides a summary of the following key aspects of the DBN Obligation under the revised PDPA:

i. **Duty to conduct an assessment of the data breach** – Once an organisation has credible grounds to believe that a data breach has occurred, it has to take reasonable and expeditious steps to determine whether the data breach is a "notifiable" breach under the PDPA within 30 calendar days, and all such steps should be properly documented. If the organisation is unable to meet the 30-day deadline, it should be prepared to explain its reasons for such failure to the PDPC, and be prepared to produce supporting evidence.

ii. **Criteria for data breach notification** – A data breach would be considered as "notifiable" under the PDPA if it is determined to be either: (a) likely to cause significant harm to the affected individuals; or (b) of a significant scale (i.e. affecting 500 or more individuals). In relation to (a), the Data Breach Guide clarifies that the Personal Data Protection (Data Breach Notification) Regulations 2021 ("**Regulation**") provides a prescribed list of personal data (or classes of personal data) that will be deemed to result in significant harm to affected individuals if compromised in a data breach. In relation to (b), the Data Breach Guide states that even if the organisation is unable to determine the actual number of affected individuals, it should still notify the PDPC once it has reason to believe that the affected number is estimated to be at least 500.

iii. **Timeframes for notification** – Once a data breach has been determined to be "notifiable", the organisation should notify: (a) the PDPC as soon as practicable, but in any case, no later than three calendar days after the organisation determines that the breach is notifiable; and (b) where required, the affected individuals as soon as practicable, either at the same time or after notifying the PDPC.

iv. **Information to be included in a data breach notification** – The organisation must provide the relevant details of the data breach to the best of its knowledge and belief, which should include the information required under the Regulation. For example, the notification to the PDPC must include the date and circumstances in which the organisation became aware of the breach; the subsequent steps taken by the organisation in chronological order; how the breach occurred; the number of individuals affected; the categories of personal data affected; the potential harm to the affected individuals, and so on. The notification to affected individuals needs to be clear and easily understood, and (amongst other things) should include information on what steps can be taken to minimise the risk of potential harm. If vulnerable individuals are involved, organisations are required to seek guidance from the PDPC on notifying the affected individuals. Other sector-specific regulators or law enforcement agencies should also be notified where required under relevant laws.

Enforcement Guide

The Enforcement Guide provides further details on the PDPC's approach in utilising its powers of enforcement in relation to handling any data privacy disputes or data breach incidents.

FACILITATION AND MEDIATION

Where a data privacy dispute arises between an individual and an organisation, the Enforcement Guide generally recommends resolving such disputes using alternative dispute resolution measures such as facilitation, mediation, etc. where appropriate. As an initial step, the PDPC may assist in facilitating communication between the parties in order to resolve the issue(s) raised. If the issues remain unresolved, the PDPC is empowered under the PDPA to refer the matter for mediation under a dispute resolution scheme, without the consent of the parties in dispute. However, should the PDPC be of the view that such facilitation and/or mediation may be inappropriate in the circumstances (e.g. where a significant amount of personal data has been leaked or where affected individuals are likely to suffer significant harm), it may instead choose to immediately commence a full investigation.

INVESTIGATION PROCESS

The Enforcement Guide also provides a brief summary of the investigation process typically carried out by the PDPC. In general, whenever the PDPC is notified of a data privacy incident, it will first determine whether the incident involves personal data. If personal data is indeed involved, it will then either: (i) refer the matter to facilitation / mediation; (ii) refer the matter to other regulatory authorities; or (iii) refer the matter to the PDPC's investigations team, depending on which option is most appropriate. In relation to (iii), the PDPC will first conduct a fact-gathering process which will involve issuing a notice to the relevant organisation to provide certain documents and information, obtaining statements, and conducting interviews and site visits. Thereafter, the PDPC will analyse all facts and information collected and subsequently issue a decision.

TYPES OF ENFORCEMENT ACTIONS

In general, where the PDPC has decided to investigate a data breach incident, it may take any of the following enforcement actions:

i. **Suspension or discontinuation** of the investigation – This will generally be considered in cases where the impact of the incident has been determined to be low. In such cases, the PDPC may also issue an advisory notice (containing certain compliance guidelines / best practices recommendations) to the organisation involved.

ii. **Allow for a voluntary undertaking** to be given – Instead of carrying out a full investigation, the PDPC is empowered to accept a voluntary undertaking in writing from the organisation involved under certain circumstances. The purpose of such voluntary undertakings is to allow organisations with clear accountability practices and remediation plans in place to be able to carry out their remediation plans for the relevant incident within a certain timeline. However, the PDPC has full discretion in deciding whether or not to allow for a voluntary undertaken to be given and, in making such decisions, the PDPC will generally consider whether the acceptance of a voluntary undertaking would result in a similar or better enforcement outcome (and in a more effective and efficient manner) as compared to carrying out a full investigation. The Enforcement Guide also provides further details on the minimum content to be included in a voluntary undertaking, and specific scenarios where the PDPC is unlikely to accept a request for a voluntary undertaking (e.g. it is a repeat incident involving a similar cause for the breach, the organisation disputes its responsibility for the incident, and so on).

iii. Issue an **expedited breach decision** – This may be considered by the PDPC in certain circumstances where it is satisfied that investigations may be completed in a significantly shorter period of time with the same enforcement outcome being achieved. In general, such circumstances include: (a) cases where the only breach of the PDPA is the fact that the organisation has failed to appoint a data protection officer or does not have a privacy policy in place; or (b) where the nature of the relevant breach is similar to precedent cases with similar fact categories (e.g. relating to poor IT governance measures, poor password policies or weak password management, personal data encrypted in ransomware incidents, etc.). Such expedited breach decisions will also be published by the PDPC, similar to regular decisions.

iv. Undertake a **full investigation process** – If after completing a full investigation the PDPC eventually determines that there has been a breach of the PDPA, the PDPC may choose to take any of the following enforcement actions: (a) issue a warning; (b) issue directions only; (c) impose financial penalties only; or (d) issue both directions and financial penalties.

When deciding whether to impose financial penalties, the PDPC will generally consider the nature of the breach and whether issuing such financial penalties is necessary to act as a deterrent (i.e. if issuing directions would be insufficient to remedy the breach or would inadequately reflect the seriousness of the breach). According to the latest revisions to the PDPA, from 1 February 2022 onwards, the maximum financial penalty that may be imposed by the PDPC will be increased to up to S$1 million or 10% of the organisation's annual turnover in Singapore, whichever higher. The Enforcement Guide also provides a non-exhaustive list of factors that the PDPC may take into account when determining the quantum of the financial penalties to be imposed, including the nature, gravity and duration of the breach, the type and nature of the personal data affected, and records of any non-compliance by the organisation in the past.

Final Thoughts

The Data Breach Guide and Enforcement Guide provide welcome guidance to organisations in Singapore seeking to understand and comply with the new obligations introduced under the revised PDPA, in particular the mandatory data breach notification obligation. Given the increase in maximum penalties (now adopting a revenue-based scale) and greater emphasis on accountability, updating or establishing a data breach management plan (including notification requirements) should be a matter of priority. Such plans should also take into account any notification requirements in other jurisdictions, since data breaches caused by cyber attacks are unlikely to only affect an organisation's Singapore office.

New Intellectual Property Arbitration Centre in Shenzhen – An Initiative to Boost Intellectual Property Protection in the Greater Bay Area

By **Amita Haylock, Partner**
Mayer Brown, Hong Kong

Jacqueline W.Y. Tsang, Associate
Mayer Brown, Hong Kong

On 20 April 2021, the China (Shenzhen) Intellectual Property Arbitration Centre (the "**IP Arbitration Centre**") opened in Shenzhen, one of the latest initiatives to foster intellectual property protection in Guangdong, Hong Kong and Macao.

Inauguration of the IP Arbitration Centre

The IP Arbitration Centre is a new division under the Shenzhen Court of International Arbitration ("**SCIA**"), established in 1983. Over the past years, the SCIA has actively promoted the development of mainland China's international arbitration within the Special Economic Zone of Shenzhen. The IP Arbitration Centre is part of the national plan to strengthen intellectual property protection, and to promote the use of alternative dispute resolution in intellectual property disputes.

The IP Arbitration Centre is strategically located in the Nanshan District. In recent years, the Chinese Government has implemented various development plans to transform the Nanshan District into a world-class innovative business centre. As more technology companies and R&D institutes settle in the area, there is an increased demand for confidential, cost-effective and speedy dispute resolution mechanism to resolve intellectual property disputes and the IP Arbitration Centre has been set up to fulfil this need. With the joint development of the Shenzhen/Hong Kong Innovation and Technology Co-operation Zone, many Hong Kong-based as well as international technology companies have opted to establish offices in the Hong Kong-Shenzhen Innovation and Technology Park at the Lok Ma Chau Loop. These companies were identified as key service targets for the IP Arbitration Centre during its opening ceremony.

Announcement of "12 Articles" on the Transformation and Application of Intellectual Property Rights in the Nanshan District

During the opening ceremony, a Nanshan District government official also announced an "Action Plan for Building an Advanced Zone for the Transformation and Application of Intellectual Property Rights (2021-2023)" (the "**Nanshan District Action Plan**"). The Nanshan District Action Plan is made up of 12 Articles, focusing on three main aspects:-

1. To foster more high-value patents – including encouraging companies in the same industry to set up "patent pools" for the purpose of sharing intellectual property rights, and providing assistance to research institutes in relation to registration and exploitation of their inventions;
2. To explore the financial aspect of intellectual property rights – including establishing an intellectual property operation fund and issuing more intellectual property securitization products to the market; and
3. To further strengthen intellectual property protection in the Greater Bay Area – including improving the intellectual property information systems and forming an anti-patent infringement alliance in the Greater Bay Area.

Conclusion

The new IP Arbitration Centre and the Nanshan District Action Plan are welcome developments in the Greater Bay Area. This signifies the Chinese Government's recognition of arbitration as an effective means of dispute resolution and a heightened awareness of intellectual property protection. Although the IP Arbitration Centre has yet to release any information on how its actual operation will differ from the SCIA, it is likely that more companies in the area will consider opting for arbitration going forward.

Arbitration (Amendment) Ordinance 2021 –

Full Implementation of the Supplemental Arrangement Concerning Mutual Enforcement of Arbitral Awards Between Mainland China and Hong Kong

By **Amita Haylock, Partner**
Mayer Brown, Hong Kong

Jacqueline W.Y. Tsang, Associate
Mayer Brown, Hong Kong

The Arbitration (Amendment) Ordinance 2021 (the "**2021 Amendment**"), which took effect on 19 May 2021, contains amendments to implement in full the Supplemental Arrangement Concerning Mutual Enforcement of Arbitral Awards between Mainland China and the HKSAR (the "**Supplemental Arrangement**"). The Supplemental Arrangement was entered into between the Supreme People's Court of China and the Hong Kong Government on 27 November 2020.

The Supplemental Arrangement

The Supplemental Arrangement was enacted to revise the existing Arrangement Concerning Mutual Enforcement of Arbitral Awards between Mainland China and the HKSAR (the "**Arrangement**"), which has been in force since 1 February 2000. The Supplemental Arrangement modified the Arrangement in four major aspects:-

1. Recognition of arbitral awards

The Supplement Arrangement expressly states that the procedures for enforcing arbitral awards under the Arrangement shall be interpreted as including the procedures for both the recognition and enforcement of the arbitral awards obtained from Hong Kong or Mainland China. This confirms that recognition is required prior to enforcing a Hong Kong award in Mainland China, which was previously a controversial issue. This approach also aligns with the international protocol of how cross-border arbitral awards are enforced. Under the Convention of the Recognition and Enforcement of Foreign Arbitral Awards (also known as the New York Convention), a two-stage approach (i.e. the recognition stage and the enforcement stage) is adopted when enforcing an arbitral award in another jurisdiction. Hong Kong is also a party to the New York Convention.

2. Extended application of interim measures

Interim measures in aid of an arbitration were not previously mentioned under the Arrangement.

Whilst the Hong Kong and Mainland China courts are empowered to grant interim relief under the Arrangement Concerning Mutual Assistance in Court-ordered Interim Measures in Aid of Arbitral Proceedings by the Courts of Mainland China and the HKSAR (which came into force on 1 October 2019) (the "**Interim Relief Arrangement**"), such interim relief can only be granted during the arbitration and before an award is made.

The Supplemental Arrangement extends the scope by allowing the relevant courts to grant interim measures (such as preservation or mandatory measures) in accordance with the law of the place of enforcement, before or after accepting an application for enforcement of an arbitral award.

3. Removal of the "Mainland arbitration authorities" restriction

Under the Arrangement, only arbitral awards made by certain recognized "Mainland arbitral authorities" could be enforced by the Hong Kong courts. The Supplemental Arrangement removes this requirement, so that all arbitral awards made in Mainland China are now enforceable in Hong Kong.

4. Provision of concurrent enforcement proceedings

Under the Arrangement, a party could not apply to enforce its arbitral award in both Hong Kong and Mainland China concurrently.

The Supplemental Arrangement removes this restriction, allowing a party to enforce an arbitral award in Hong Kong and Mainland China simultaneously, subject to the condition that the total amount to be recovered in the two jurisdictions must not exceed the amount determined under the arbitral award. The court in one place of enforcement shall, at the request of the court of the other place, provide information on the status of the enforcement proceedings. This is to avoid double recovery by a party bringing concurrent enforcement actions in Hong Kong and Mainland China.

2021 Amendment

In Mainland China, the Supplemental Arrangement was implemented via a judicial interpretation released on 27 November 2020.

In Hong Kong, revisions 1 and 2 as set out above came into effect on 27 November 2020, while revisions 3 and 4 required amendments to the Arbitration Ordinance (Cap. 609) in order to be implemented. For this purpose, the 2021 Amendment was enacted and came into effect on 19 May 2021. Pursuant to the 2021 Amendment,

- the requirement that "only awards made by certain recognized 'Mainland arbitral authorities' is enforceable" is deleted from the Arbitration Ordinance – and so all arbitral awards made in Mainland China are now enforceable in Hong Kong; and
- section 93 of the Arbitration Ordinance is repealed – and so a party who obtains an arbitral award in Mainland China can now concurrently enforce the award in both Hong Kong and Mainland China.

Conclusion

The Supplemental Arrangement is now finally implemented in full in Hong Kong. It is expected that the 2021 Amendment will bolster the mutual legal co-operation between Mainland China and Hong Kong, and further strengthen Hong Kong's position as the preferred seat of arbitration to resolve disputes involving parties or assets in Mainland China.

China - A New 'Special Action Plan' to Crack Down on Bad Faith Trade Mark Registrations

By **Gabriela Kennedy, Partner**
Mayer Brown, Hong Kong

Michelle Yee, Counsel
Mayer Brown, Hong Kong

Introduction

In line with the Chinese government's recent push to crack down on trade mark hijacking, the China National Intellectual Property Administration ("**CNIPA**") announced a 'Special Action Plan for Combating Bad Faith Trade Mark Hijacking' (打击商标恶意抢注行为专项行动方案)[36] ("**Special Action Plan**") on 24 March 2021.

Background

The Special Action Plan is the latest in a series of measures introduced by the Chinese government to discourage and tackle bad faith trade mark applications in recent years, such as amendments to the Trade Mark Law and the implementation of "Several Measures for Regulating Applications to Register Trade Marks" ("**2019 Measures**") that took effect in November and December 2019, respectively.

The Special Action Plan aims to crack down on various types of "bad faith behaviour" relating to the improper use of the Chinese

36 Full text (in Chinese) found at: https://www.cnipa.gov.cn/art/2021/3/24/art_75_157972.html.

trade mark registration system through coordinated action and information sharing amongst trade mark authorities at the regional, provincial and national levels, and the application of consistent examination standards in administrative and judicial enforcement proceedings.

What Kind of Behaviour will be Targeted Under the Special Action Plan?

The Special Action Plan sets out 10 categories of targeted bad faith behaviour, namely:

1. bad faith registration of the names of national or regional strategic plans, major events and policies, or important scientific and technological projects;
2. bad faith registration of words and signs relating to natural disasters, serious accidents, major public health or social security incidents, or other public emergencies, which harm public interests;
3. bad faith registration of the names and logos of important competitions or exhibitions of significant repute;
4. bad faith registration of the names of administrative divisions, rivers and mountains, scenic attractions, buildings, or other public resources;
5. bad faith registration of common names for goods and services, industry terms, or other public commercial resources;
6. bad faith registration of the names of well-known public figures, renowned works or characters;
7. bad faith registration of third party trade marks or other commercial signs that are relatively well-known or distinctive, which damage that third party's prior rights and interests;
8. clear contraventions of Article 10 of the Trade Mark Law, or violations of public order and customs, which have a serious detrimental impact on the political, economic, cultural, religious, ethnic, or other social public interests of China;
9. improper acceptance of instructions by trade mark agencies, where they know or should know that their client is engaging in the above bad faith behaviour, or other improper behaviour that disrupts the trade mark registration process; and
10. other clear violations of the principles of honesty and good faith.

The above categories of targeted behaviour elaborate on the existing statutory provisions targeting bad faith filings under the Trade Mark Law and the 2019 Measures. For example, category 5 loosely corresponds to Article 11 of the Trade Mark Law, which prohibits the registration of common, generic, or purely descriptive signs, or signs that are otherwise not distinctive, whereas category 7 covers similar ground as Article 32 of the Trade Mark Law, which prohibits the pre-emptive bad faith registration of an existing third party trade mark that has attained a certain degree of influence. The specific reference to '*words and signs relating to major public emergencies*' may have been triggered by a spate of applicants seeking to register COVID-19-related trade marks during the height of the pandemic.[37]

The behaviour of trade mark agencies is also explicitly mentioned as a separate category, which is in line with existing statutory provisions in the Trade Mark Law and the 2019 Measures holding trade mark agencies accountable for their role in trade mark hijacking activities.[38] This category addresses situations where trade mark agencies facilitate the clear bad faith behaviour of clients, although there is no specific reference to cases where a trade mark agency is affiliated with a hijacker or where an agency seeks to hijack the marks of their clients.[39]

The final category serves as a catch-all provision to cover bad faith behaviour not specifically addressed by the preceding categories, and which echoes the wording of paragraph 1 of Article 7 of the Trade Mark Law ('*use and registration of trade marks should conform with the principles of honesty and good faith*'). Given the myriad ways in which bad faith filers seek to hijack third party trade marks, it

37 For examples of such enforcement action, see: http://sbj.cnipa.gov.cn/gzdt/202002/t20200227_312227.html ; http://sbj.cnipa.gov.cn/tzgg/202003/t20200304_312498.html

38 See in particular Article 19 of the Trade Mark Law.

39 The latter types of behaviour are specifically addressed in Articles 15 and 19 of the Trade Mark Law. Sanctions for trade mark agencies that engage in or facilitate bad faith filings are set out in Article 68 of the Trade Mark Law and Articles 13 and 15 of the 2019 Measures.

would be hard to argue against the necessity of such a catch-all provision. However, there is a risk that such broad and vaguely defined wording could be construed in ways that could lead to the rejection of filings made by legitimate brand owners (for example, would a filing made by a brand owner for defensive purposes with no genuine intent to use be considered to be made in bad faith?).

What Are the Main Aims of the Special Action Plan?

The Special Action Plan specifies five areas that it aims to strengthen, including: (1) investigation and evidence gathering; (2) targeted strikes; (3) cooperation between departments; (4) comprehensive policy implementation; and (5) publicity and education.

Strengthening investigation and evidence gathering involves a review by each regional authority on the implementation of the Special Action Plan at a local level to determine the appropriate focus of work and provide an accounting of work done, and to ensure that the quality of evidence gathered for trade mark hijacking cases is detailed, comprehensive, and complete.

Targeted strikes involve coordinated action throughout the trade mark registration process to identify and reject hijacked marks. This includes proactive monitoring and information sharing by the relevant agencies on bad faith filing activity, the implementation of rapid-rejection mechanisms where appropriate, and consistent enforcement at each stage of the registration and post-registration process. Whilst the Special Action Plan does not specifically refer to the CNIPA's internal blacklist, blacklisting would be one way to ensure that any applications or registrations made by identified hijackers would be rejected, whether during substantive examination or in the course of opposition / invalidation proceedings.

The Special Action Plan encourages coordination between the CNIPA, administrative authorities and the courts to align examination and enforcement standards, and emphasises the comprehensive implementation of deterrents and punitive measures (including legal penalties, administrative guidelines and credit restrictions[40]) against trade mark hijackers and agencies that facilitate hijacking activity. It also calls for the elimination of quotas as a performance metric for trade mark examiners, presumably to encourage examiners to scrutinise applications more carefully to identify bad faith behaviour. The elimination of quotas is welcome news for brand owners and trade mark practitioners, many of whom have been frustrated in recent years by inconsistent and at times completely unreasonable rejections of trade mark applications by inexperienced and overworked examiners.

Lastly, government agencies are instructed to promote their increased efforts to target and penalise trade mark hijacking activity, and to publicise high-profile cases to educate the general public and deter bad actors.

Stages of Implementation

The Special Action Plan will be implemented in three phases:

- Phase 1: Mobilisation and Deployment (March 2021);
- Phase 2: Organisation and Implementation (April-October 2021); and
- Phase 3: Summary and Supervision (November-December 2021).

MOBILISATION AND DEPLOYMENT (MARCH 2021)

This phase involves promoting the Special Action Plan to raise public awareness, setting primary objectives, creating work plans, mobilising and deploying appropriate personnel to achieve those objectives. The emphasis is primarily on the gathering of evidence, to be carried out by regional intellectual property departments and collated by their respective provincial intellectual property offices. For pending trade mark applications, the work would be carried out by local trade mark examination and cooperation centres. The collected evidence will be submitted to the CNIPA Trade Mark Office ("**TMO**") to be organised and redistributed to different departments for follow-up action.

40 Credit restrictions may include entering details of bad faith filers into the National Public Credit Information System, which would allow other agencies to impose disciplinary measures.

ORGANISATION AND IMPLEMENTATION (APRIL-OCTOBER 2021)

During this phase, evidence gathered during the previous phase will be examined and actioned by various intellectual property departments. Evidence relating to pending trade mark applications will be reviewed by local trade mark examination and cooperation centres under the TMO's supervision. For cases involving trade marks under opposition or invalidation proceedings, the TMO will review the relevant evidence.

For high-profile trade mark hijacking cases, or cases involving major public emergencies, the Department of Intellectual Property Protection will transfer the gathered evidence to the relevant regional intellectual property departments for review. Evidence relating to administrative decisions, adjudications or court judgments in which trade mark agencies have been found to engage in bad faith behaviour will be referred by the Department of Intellectual Property Utilization and Promotion to local intellectual property law enforcement departments for investigation and follow-up.

SUMMARY AND SUPERVISION (NOVEMBER-DECEMBER 2021)

The final phase of the Special Action Plan involves the inspection and supervision by the TMO of work done by local trade mark examination and cooperation centres. The provincial intellectual property offices will also review the implementation of the Special Action Plan within their jurisdictions. Summary reports from the various local trade mark examination and cooperation centres and provisional intellectual property offices are to be submitted to the TMO before 10 December 2021 for evaluation and dissemination.

This will be an important evaluation stage for the Special Action Plan, given that the actual implementation will be driven by local examination centres and provincial intellectual property offices. The consolidation and evaluation of results from the various local offices may provide useful information on the effectiveness of the measures implemented, and shed light on emerging trends or new types of bad faith behaviour.

Conclusion

With the introduction of the Special Action Plan, the Chinese government is signalling its renewed commitment to protecting intellectual property rights and its intention to reverse its reputation as a haven for trade mark hijackers and counterfeiters. Compared with other recent legislative and regulatory measures targeting bad faith filings such as the 2019 Measures, the Special Action Plan takes a holistic approach, with an emphasis on consistent examination and enforcement standards and coordinated action amongst intellectual property authorities at the national, provincial, and regional levels.

The Special Action Plan is currently in its second phase (Organisation and Implementation), and many provincial intellectual property offices and local trade mark examination and cooperation offices have already issued instructions on implementing the Special Action Plan.[41] Given the Special Action Plan has a finite term of around 9 months, there are understandably concerns that it will only be a series of short-term fixes with no lasting impact beyond 2021; it is hoped that the overall evaluation to be conducted by the TMO at the end of Phase 3 will yield useful lessons that can lead to long-term measures for efficient and effective targeting of trade mark hijacking and a more robust intellectual property protection system going forward.

*The authors would like to thank **Joanne Cheung**, Trainee Solicitor at Mayer Brown, for her assistance with this article.*

41 For example, Shanghai: http://sipa.sh.gov.cn/xxgkml/20210513/84d667957b9f459498a30beb0a8d5cab.html; Guangdong: https://www.gippc.com.cn/ippc/ywzx2/202104/568704394a404828b76ad541040f0fd0.shtml

Contact Us

Gabriela Kennedy
Partner
+852 2843 2380
gabriela.kennedy
@mayerbrown.com

Amita Haylock
Partner
+852 2843 2579
amita.haylock
@mayerbrown.com

Karen H. F. Lee
Counsel
+65 6327 0638
karen.hf.lee
@mayerbrown.com

Michelle G. W. Yee
Counsel
+852 2843 2246
michelle.yee
@mayerbrown.com

Jacqueline W. Y. Tsang
Associate
+852 2843 4554
jacqueline.tsang
@mayerbrown.com

Cheng Hau Yeo
Associate
+65 6327 0254
chenghau.yeo
@mayerbrown.com