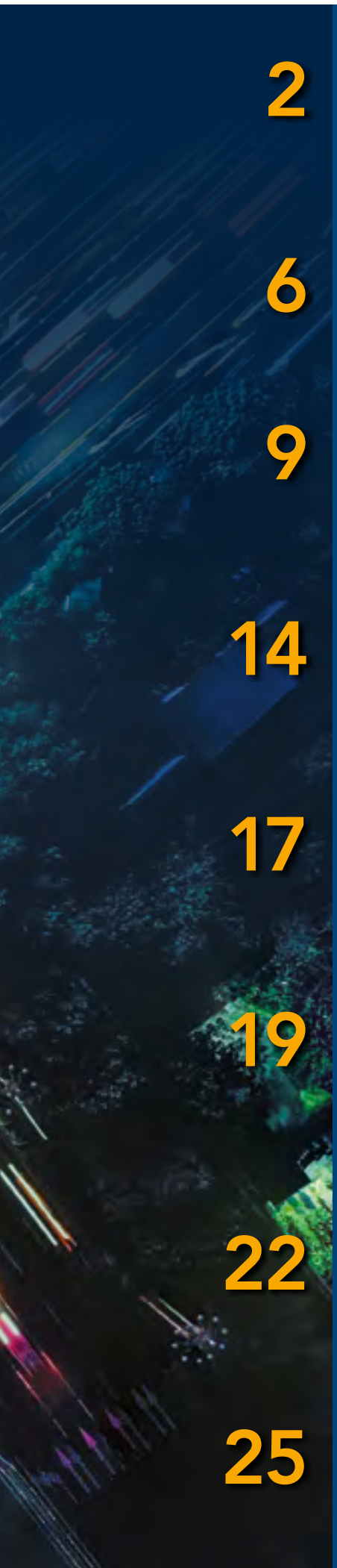
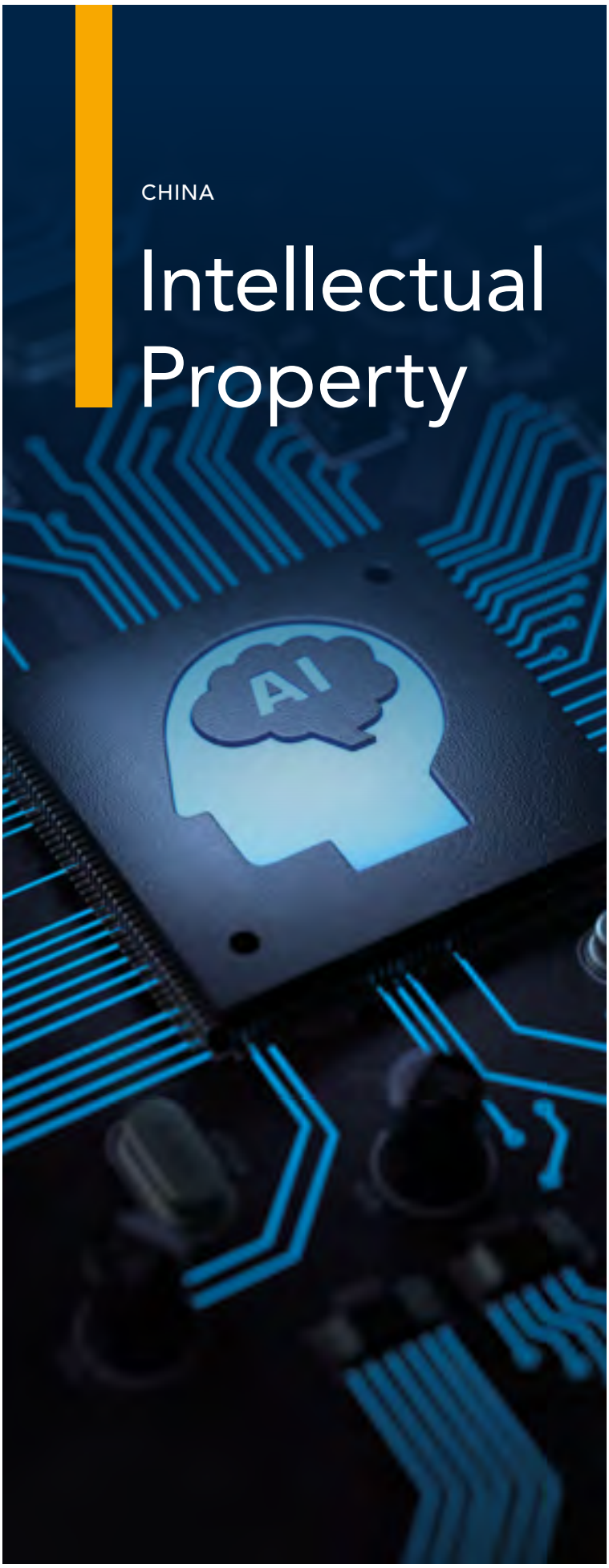
MAYER | BROWN

IP & TMT Quarterly Review

First Quarter 2020

Contents





Chinese Courts Rule on Whether Copyright Subsists in AI-generated Works

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

The increased use of artificial intelligence ("**AI**") in artworks, music and literary works has prompted an interesting debate around whether AI-generated works enjoy copyright protection. And, if so, is the unauthorised copying of an AI-generated work permissible?

Recently, two courts in the People's Republic of China ("**PRC**") considered these questions for the first time – and came up with differing views, demonstrating that the issue is complex and far from settled.

Feilin v Baidu (April 2019)[1]

In this case, the Beijing Internet Court ("**BIC**") considered whether copyright protection should extend to a report generated with the assistance of an AI-powered software.

On 9 September 2018, Beijing Feilin Law Firm ("**Feilin**") published a report about the Beijing courts' decisions in relation to the film industry ("**Report**") on its public WeChat account. The Report had been created with the help of "Wolters Kluwer China Law and Reference", a legal online database underpinned by an intelligent technology platform ("**Software**").

1 *Beijing Feilin Law Firm v Baidu Wangxun Co., Ltd.*, Beijing Internet Court, (2018) Jing 0491 Min Chu No. 239.

According to Feilin, the Report was created as follows:

1. Feilin's employees searched the Software for Beijing court judgments during a specified period, using the keyword "film";
2. The Software's visualisation function was then applied to generate a preliminary report with charts and text, detailing information such as the total number of Beijing court judgments concerning the film industry, as well as outcome, court type and judges; and
3. The Report was then created by editing the charts, removing irrelevant search results and writing an analysis based on the statistics in the preliminary report.

The following day, the Report was reposted on an online platform hosted by Baidu Wangxun Co., Ltd., part of Chinese tech giant Baidu ("**Baidu**"), and Feilin's name, which was originally on the Report, had been removed. Feilin claimed that Baidu published the Report without authorisation, and contravened, among other things, its right to disseminate information on networks as a copyright owner. In its defence, Baidu contended that the Report, as a whole, was created automatically by the Software and fell outside the scope of copyright protection since it lacked originality and was not an intellectual creation.

RELEVANT LAW

According to the Copyright Law of the PRC and the Regulations for the Implementation of the Copyright Law of the PRC ("**Regulations**"), a "work" protectable by copyright (including literary work) must be:

1. An intellectual creation;
2. Original; and
3. Capable of being reproduced in a tangible form.

Here, the core issues were whether the Report was original and whether it was an intellectual creation.

JUDGMENT

(i) The question of copyright in the final Report

The BIC compared the Report and the preliminary report as automatically generated by the Software's "visualisation" function, and found various differences. Accordingly, the BIC held that the Report was independently created by Feilin's employees and was original, thus qualifying as a literary work protected by copyright. Since Baidu had uploaded the Report on its platform without Feilin's consent, the BIC ordered Baidu to pay Feilin damages of RMB1,560 and publish a statement of apology.

(ii) The question of copyright in the preliminary report

However, what is interesting is that the BIC went on to consider whether copyright also subsisted in the preliminary report automatically generated by the Software's "visualisation" function.

The BIC first found that the text of the preliminary report was sufficiently original since it reflected selection, judgment and analysis of data related to Beijing court judgments concerning the film industry.

Nevertheless, the BIC held that, even if a work is considered original, it would only attract copyright protection if it is the intellectual creation of a natural person. In the present case, while the Software automatically generated the text of the preliminary report, human participation occurred in two stages of the creation process – the software-development stage and the software-use stage. The BIC found that neither the software developer nor the software user (i.e. the Feilin employee) could be said to be the author of the preliminary report. As the software developer did not input the specific search criteria which led to the generation of the preliminary report, there was no original idea or emotion passed on to the report. As for Feilin's employees, although they conducted the keyword search, this act alone was insufficient to pass on their original ideas and emotions.

Accordingly, even though the preliminary report was original, it did not constitute a literary work since it was not an intellectual creation.

Although the preliminary report did not attract copyright protection, the BIC recognised that it deserved some other form of protection. Unfortunately this was not specified by the BIC.

COMMENTS

The BIC's ruling shows that while works created with the help of AI may qualify as copyright protectable works (depending on the extent of human intervention), a purely AI-generated work without

human intellectual input will not be protected. It also shows that the development and the application of an AI software (e.g. setting the search criteria) would not constitute the required intellectual activities for a finding of copyright protection.

By contrast, the Shenzhen Nanshan District People's Court ("**Shenzhen Court**") reached a different conclusion in *Tencent v Yingxun*[2] in December 2019. It essentially came to the conclusion that a purely AI-generated article may qualify as a literary work protected by copyright.

Tencent v Yingxun (December 2019)

In 2015, Tencent Technology (Beijing) Ltd developed its Dreamwriter software, an automated writing software, and licensed it to Shenzhen Tencent Computer System Co. Limited ("**Tencent**"). Tencent applied the Dreamwriter software to produce around 300,000 articles each year. On 20 August 2018, Tencent published an article on its website which analysed stock market data on that day ("**Article**"), with a remark that it was "*automatically written by Tencent's robot, Dreamwriter*".

Tencent claimed that the Article was written and published according to the following process:

1. The Dreamwriter software collected historical and real-time stock market data and analysed the data through machine learning;
2. It then assessed whether the analysed data met certain conditions prescribed to trigger the generation of an article;
3. Once the condition was met, it wrote the Article on the basis of the data, according to an article template; and
4. It proofread the Article and uploaded the Article on Tencent's online platforms.

The whole process, from data collection to uploading, was done automatically by the Dreamwriter software, in just two minutes after the stock market closed. However, prior to this, Tencent's employees were responsible for selecting the data input criteria, the trigger conditions and the template for the structure of the Article etc. of the Dreamwriter software.

The Article was subsequently reposted by Shanghai Yingxun Technology Company ("**Yingxun**") on its website without Tencent's consent. Tencent contended that Yingxun infringed a number of its rights including the right to disseminate information on networks. Yingxun argued copyright did not subsist in the Article, being a purely AI-generated work.

JUDGMENT

As with the BIC, the Shenzhen Court had to determine whether the Article was original and an intellectual creation.

It first found that the Article was sufficiently original since its content reflected selection, analysis and judgment of the stock market, and was presented clearly and logically. Departing from the *Feilin* judgment, the Shenzhen Court found the Article to be an intellectual creation since it reflected the individual choice and judgment of Tencent's employees, who were responsible for setting the data input criteria, the trigger conditions and the article template, etc. of the Dreamwriter software. In the Shenzhen Court's view, the Dreamwriter software merely performed the technical function of generating the Article in accordance with the desire of Tencent's employees.

As such, the Article constituted a literary work protectable by copyright. The Shenzhen Court found that Tencent was the author and copyright owner of the Article, and awarded Tencent RMB1,500 as damages for Yingxun's infringement of Tencent's copyright.

Takeaway

The *Feilin* and *Tencent* judgments make it clear that both originality and human intellectual activities are necessary conditions of copyright protection. This is no surprise as these requirements are clearly stated in the Copyright Law of the PRC and the Regulations, and are likewise recognised in other jurisdictions.

What is intriguing is that the two courts differed in their application of the requirement of "intellectual creation". The Shenzhen Court in Tencent found that the Article was an intellectual creation in view of the involvement of Tencent's employees in the

2 *Shenzhen Tencent Computer System Co. Limited v Shanghai Yingxun Technology Company*, Shenzhen Nanshan District People's Court, (2019) Yue 0305 Min Chu No. 14010.

application of the Dreamwriter software (e.g. selecting search criteria and templates), whereas the BIC in *Feilin* held that similar involvement by Feilin's employees was insufficient to convey their original choices and judgment to the preliminary report.

Precedents are not binding in the PRC, but what is clear from the two cases is that the greater the human involvement in the creation of an AI-generated work, the more likely it will be recognised as a copyright-protectable work. Nonetheless, an AI-generated work with no human involvement will not attract copyright protection.

Conclusion

The issue of how AI-generated works are to be legally protected has emerged as a topic of discussion among intellectual property lawyers globally. The International Association for the Protection of Intellectual Property (AIPPI) recently resolved that AI-generated works may qualify for copyright protection only if there is human input in the creation of the work. The World Intellectual Property Organization (WIPO) is also considering this issue in a public consultation process which has ended recently. Finally, legal issues associated with AI may also go beyond copyright law – the European Patent Office and the UK Intellectual Property Office have recently ruled, for the first time, that an inventor of a patent must be a natural person, and rejected patent applications which described the inventors as AI programmes.

*The author would like to thank **Christopher C. H. Ng**, trainee solicitor at Mayer Brown, for his assistance with research for this article.*

Facial Recognition – New PRC Guidelines

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

Cheng Hau Yeo, Associate
Mayer Brown, Singapore

Introduction

On 18 February 2020, China's Special App Governance Working Group ("**Working Group**") issued guidelines on the collection of facial recognition data by app operators in China ("**Guidelines**"). According to the Working Group, the Guidelines were issued in light of growing concerns stemming from the increasingly ubiquitous use of facial recognition in China. The risks of abuse are evident – for example, there have been reports of schools using facial recognition technology to monitor students' behaviour during lessons. Recently, a group of criminals had reportedly managed to deceive the Alipay facial recognition system using 3D avatars. Despite these risks, facial recognition technology is still being widely used in China due to its numerous benefits, such as improving the flow of foot traffic at airports and train stations, making online services more secure through remote identity verification, and more recently, some organisations have been using facial recognition to conduct identity checks to safeguard against the spread of COVID-19.

Background

According to the Guidelines, the Working Group received more than 500 complaints on its personal data reporting platform, relating to facial recognition involving over 50 apps ("**Complaints**"). The Complaints include apps using facial recognition for

identity checks, generating virtual faces via AI, predictive analysis and so forth. Most of the apps claimed to have used facial recognition to conduct identity checks so as to avoid credibility issues associated with traditional identity verification methods such as the use of names, phone numbers and identity document numbers. Currently, facial recognition is being used in authentication processes for transactions such as opening financial accounts, processing online payments, and verifying memberships.

Analysing Common Phenomena and Issues

Approximately 60% of the apps reported in the Complaints made it mandatory for users to provide their facial information in order for them to receive relevant services. Most of these apps justified their use of facial recognition by citing the need to comply with applicable laws or industry regulations to reduce business and fraud risk. Facial data is considered by app operators as a safer method of ascertaining identity as compared to traditional verification methods such as collecting photos and identity documents. However, according to the Guidelines, the consequences of any unauthorised access to facial data are potentially more serious as the verification process captures photos of the individual's face from every angle.

In addition, around 90% of the apps did not provide clear and sufficient information to users regarding the collection, use and storage of facial data. The Working Group found that most of the apps only included a simple statement within their privacy policy that users' personal data would be retained for the maximum period prescribed by law and would subsequently be anonymised upon expiry of this period. However, no further information was provided in relation to the collection, use and storage of facial data, such as the scope of such collection and use, whether images would be disclosed to a third party and any security measures taken. Furthermore, requests from users for further information relating to the collection, use and storage of their facial data were occasionally met with refusals from the relevant app operator on the ground of protection of trade secrets.

Most significantly, the Working Group found that almost all of the apps reported in the Complaints failed to provide a clear and effective mechanism (if any) for the withdrawal of users' consent. Upon contacting the customer services teams for the relevant apps, some of the users discovered that there was in fact no consent revocation mechanism in place for these apps. An effective mechanism for the withdrawal of consent to the collection, use or storage of personal data is crucial.

In such circumstances, app operators have argued that users may simply cease using the facial scanning function of the app (for example, to effect payment through e-payment apps) if they wish for the app operator to stop using their facial data. In reality, the app operators would continue to store the facial data for subsequent use in the future in case they might need to authenticate the user's identity again via facial recognition. The Working Group's view was that this may not constitute an effective revocation of consent as facial data is arguably no longer necessary post-identity authentication and users should be provided with a clear mechanism for withdrawing consent to the use and storage of their facial data by these app operators.

The Guidelines

Given all the issues identified in the Complaints, the Working Group has recommended that app operators adopt the following eight measures:

1. Ensure that the purpose of collection of facial data is lawful, proper and necessary. In particular, app operators should consider collecting facial data only when it is in the interest of users or when it is necessary to fulfil specific regulatory requirements. Facial recognition should not be made a mandatory prerequisite for users to receive the services provided under the app.
2. Provide a separate notification to users relating to the purpose, method, scope and retention period of facial data collection and any other information which may be of interest to them. Such information should be provided in the app's privacy policy as well. Explicit consent should be obtained from users before any collection of their facial data.
3. Facial data should not be stored by the app operators. Identity verification should be conducted directly via collection terminals, which can carry out authentication without the need to store facial data. Should an external server be required to first process the data, all

images from which facial data can be extracted should be deleted immediately after identity authentication.

4. Adopt measures such as encrypted transfer and storage and implement strict controls and auditing measures to ensure the security of the data collected via facial recognition.
5. Cooperate with the relevant authorities such as the Public Security Bureau when using facial data for identity verification.
6. Improve the procedures through which users can exercise their rights in relation to their facial data, such as the ability to enquire about the state of collection and use, revoke their consent to collection and find out whether the app operator has stored their data.
7. Avoid disclosing or transferring facial data collected to third parties without the consent of the relevant users.
8. Consider using facial recognition as more of a supporting mechanism so as to strike a balance between convenience and security, for example, for small-scale payments and fast-track processing.

Takeaways

Facial recognition is a fast-growing field in China. The technology is increasingly permeating all corners of society, from payments to security control in public transportation hubs and even in schools. Despite its prevalence, there is little to no legal guidance specifically relating to its use in China. Therefore, the Guidelines represent a welcome first step towards establishing a regulatory basis for such collection and striking a balance between convenience and security. While the Guidelines are not legally binding, they are likely to serve as a useful guide for Chinese authorities in their enforcement of China's Cybersecurity Law and therefore app operators should strive to comply with them as far as practicable when collecting, using or storing facial data.

Out with the Old, In with the New: Proposal for Review of the Personal Data (Privacy) Ordinance

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

Cheng Hau Yeo, Associate
Mayer Brown, Singapore

Introduction

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 last underwent amendment 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 needs of the digital age, the PDPO has seen no amendment 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 in direct reaction to specific events in Hong Kong which 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 amendments are a nod in the direction of international developments, such as the mandatory breach notification proposal.

Key Recommendations

(I) 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 the data subjects can be identified and there is a reasonably foreseeable risk of harm by 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; this may hinder timely follow-up actions.

At the same time, mandatory data breach notifications have become the international norm – the EU, Australia, Canada, the PRC, Taiwan, the Philippines and South Korea 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, however, now 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: (i) a definition of "personal data breach"; (ii) a notification threshold; (iii) a timeframe for notification; and (iv) a format for the notification. These elements are discussed below:

a. **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*";

b. **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;

c. **The timeframe for notification**: data users are required to make notifications within a specified timeframe (e.g. no later than five business days when 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; and

d. **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 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-hour 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.

(II) 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 fulfillment 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.

(III) 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.

(IV) 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.

(V) 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 4,700 doxxing cases since 14 June 2019 and has referred more than 1,400 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 of the PDPO 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.

(VI) 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$1,000 if the offence continues). However, so far, Hong Kong courts have only issued fines between HK$1,000 to HK$5,000 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 – it seeks to align Hong Kong 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.

*The authors would like to thank **Christopher C. H. Ng**, trainee solicitor at Mayer Brown, for his assistance with research for this article.*

All Together: Recent Collaboration Initiatives on Data Privacy and Cybersecurity

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

Cheng Hau Yeo, Associate
Mayer Brown, Singapore

Background

Hong Kong's privacy regulator, the Privacy Commissioner of Personal Data ("**PCPD**"), is in discussions with the UK's Information Commissioner's Office ("**ICO**") to enter into a memorandum of understanding ("**MoU**") in 2020. This comes on the heels of another MoU signed by the PCPD with its Singapore counterpart last year. In addition, the PCPD is also contemplating a similar move with countries such as Australia and Canada. Within the Asia-Pacific region, several MoUs relating to cybersecurity and data privacy cooperation have recently been entered into between countries such as Australia, Hong Kong, India, Indonesia and Singapore. Apart from such cross-border collaboration, regulators and government agencies within Hong Kong have also recognised the need for stronger inter-organisational collaboration.

This article will highlight some of the key points in these MoUs, including the MoU entered into between Hong Kong and Singapore in 2019 against the background of past data breaches in Hong Kong such as the TransUnion Hong Kong data breach

incident, which shed light on the interface amongst antitrust, consumer and data protection and emphasises the importance of stronger collaboration between government agencies across different disciplines and countries.

The Hong Kong-Singapore MoU

In May 2019, the PCPD and the Personal Data Protection Commission of Singapore ("**PDPC**") signed a MoU to strengthen their mutual cooperation and share knowledge on potential and ongoing data breaches. While Hong Kong was one of the earliest jurisdictions in Asia to introduce a comprehensive data privacy law in 1996, Singapore's equivalent took effect in 2012. As the Singapore data protection law was enacted at a much later date than the Hong Kong statute, the PCPD noted that Singapore's Personal Data Protection Act 2012 is more mature and up-to-date as compared to the Personal Data (Privacy) Ordinance in Hong Kong. The PCPD further noted that due to its status as a direct government department, Singapore's PDPC has been able to propose initiatives more quickly as compared to the PCPD. Therefore, Hong Kong has been able to observe and learn from how certain studies and initiatives have panned out in Singapore.

Since their entry into the MoU last year, both parties have jointly developed and released a Guide to Data Protection by Design for ICT Systems ("**Guide**") which aims to encourage organisations to consider data protection issues at the design stage and offers practical guidance to organisations on each phase of their software development as well as robust data protection measures for ICT systems. Currently, the "data-protection-by-design" concept is not a mandatory requirement (unlike in the EU) but is nevertheless recommended by both the PCPD in Hong Kong and PDPC in Singapore. The Guide's key principles include transparency, user-centricity and data minimisation, i.e. only collecting data relevant and necessary for its purpose. In addition to the Guide, the PCPD recently noted that both parties have been working on another four to five projects, with half of them relating to artificial intelligence and FinTech.

Given the number of high profile data breach incidents that have occurred in both Hong Kong and Singapore over the past two years, the MoU allows the parties to learn from each other's experiences and be better equipped to deal with similar incidents in future. Examples of these incidents include the SingHealth data breach incident in 2018, during which the Singapore cluster of public healthcare institutions suffered the "most serious breach of personal data" in Singapore's history which affected 1.5 million individuals. In the same year, Cathay Pacific, a Hong Kong-based airline, also suffered a major data breach incident affecting 9.4 million users.

Other MoUs on Cybersecurity and Data Protection in Asia Pacific

The Cyber Security Agency of Singapore has signed several MoUs on cybersecurity cooperation with Australia, Canada, France, India, the Netherlands, the UK and the US, a Joint Declaration with Germany and a Memorandum of Cooperation with Japan. India has signed a MoU with Canada in 2015, with the UK in 2016 and with the US Computer Emergency Readiness Team (US-CERT) in 2017 among others. More geographically far-reaching cooperation include Taiwan and St. Lucia. These MoUs mostly involve bilateral or multilateral cybersecurity cooperation. For example, the MoU entered into between Singapore and Canada in 2018 covers areas such as exchanging information on cyberattacks and threats, providing technical and certification services, and collaborating to enhance regional cybersecurity capacity. Other areas of cooperation commonly seen in these MoUs include the exchange of ideas relating to regulations and national policies to promote the digital economy, managing responses to cyber threats, sharing information on cyber threats, and even supporting cybersecurity capacity development via training programmes and awards (such as scholarships for professional education programs).

Inter-Organisational Collaboration – Intersecting Prisms of Data Protection, Consumer Interests and Antitrust Enforcement

In 2018, the Hong Kong arm of consumer credit reporting agency TransUnion suffered a widely-publicised data breach, which impacted 5.4 million consumers in Hong Kong. Following this data breach incident, Hong Kong's PCPD has arranged meetings with the city's Competition Commission and Consumer Council to explore ways in which these the agencies can collaborate given the interface between antitrust, consumer, and data protection issues.

Through TransUnion's simple online authentication process, a local newspaper managed to gain access to the personal data of the city's public figures, including the Chief Executive and the Financial Secretary. TransUnion, the primary supplier of data to Hong Kong's top 10 banks and some 140 financial institutions, arguably should have very strong security around the financial data of individuals in Hong Kong. From a data protection perspective, TransUnion is an obvious target for cyberattacks or data breaches given the volume of data it holds. From an antitrust perspective, the monopolistic nature of TransUnion in the industry does not bode well for consumers, especially as most of the city's top banks and financial institutions rely on it for its credit reporting services. A review of the TransUnion data breach would have benefitted from an examination from an anti-trust perspective and not just from a data protection point of view.

Takeaways

Cybersecurity and data protection are becoming cross-border issues, given that the daily use of data by large organisations involves the transmission and processing of such data on a multi-jurisdictional basis. Very few companies isolate data and have uses of it that are purely local. Given the ever evolving digital landscape in Asia and intensifying cyber risks, strong international partnerships are key to navigating an increasingly complex, data-dense cyber terrain. Cross-border inter-organisational collaborations are becoming crucial and MoUs provide the fundamental legal basis for countries to achieve global interoperability and build mutual understanding for better enforcement against cyber-attacks and data breaches. As data breaches become more sophisticated and have legal implications that go beyond the realm of data protection legislation alone, there is also a growing need for regulators and government agencies across different disciplines to work with each other to gain a fuller understanding of data breaches and identify legal issues from various perspectives where necessary.

China Introduces New Advertising Rules for the Pharmaceutical Industry

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

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

The Interim Administrative Measures on the Review of Drugs, Medical Devices, Dietary Supplements and Food for Special Medical Purpose (FSMP) Advertisements (the "**Measures**") came into force on 1 March 2020. The Measures signify a major regulatory development for pharmaceutical advertising, as they consolidate various administrative measures applicable to Drugs, Medical Devices, Dietary Supplements and Food for Special Medical Purpose ("**FSMP**") into one regulation. The enactment of the Measures also shows the continuous effort China is making to standardise pharmaceutical advertising activities, and to curb false and misleading advertising.

Scope of Application

The Measures introduce a review and approval process for all drugs, medical devices, dietary supplements and FSMP advertisements, with an exemption for advertisements that only promote or publicise the name of the product.

Simplified Application and Review Process

While the State Administration for Market Regulation (SAMR) has been tasked with enforcing the Measures, the examination of

advertisements will be carried out by the local advertising examination authorities (i.e. The Department of Administration for Industry and Commerce and the Department of Medical Products Administration in each province, autonomous region, and direct-administered municipality).

Applicants making an application for the review of advertisements will need to submit to the authorities the following: a simplified set of documents, including the application form, copy of the advertisement, registration documents of the applicant, registration certificate of the product, product labels, instructions for use, and documents certifying the intellectual property involved in the advertisement.

The examination process has to be completed within 10 days and if approval is granted, an advertisement approval number will be issued. The authorities are required to make public the information relating to approved advertisement applications (such as the advertisement approval number and the applicant's name, etc.) on their official website or through other means.

Mandatory Content for Advertisements

Advertisements for drugs, medical devices, dietary supplements and FSMP shall not contain any false or misleading information. Advertisers shall ensure the authenticity and legality of the advertising content.

The Measures also stipulate the content and information that have to be included in such advertisements. For example, all drug advertisements are required to contain information on contraindications, side effects and the advertisement approval number. Advertisements for non-prescription drugs should include the over-the-counter (OTC) logo as well as a cautionary statement "please consult a pharmacist before purchasing and using this product". For prescription drugs, advertisers should include the following statement - "it is intended for medical and pharmaceutical professionals only". The advertisement approval number has to be included in the advertisement together with the mandatory content which must be displayed in the advertisement at all times and in a prominent manner in an "easily discernible" font and colour.

The Measures also introduce certain prohibitions which relate to drugs, medical devices, dietary supplements and FSMP advertisements. Advertisers are not allowed to use the name or image of any state authority or any of its staff member to promote their products or devices.

Contraventions of the Measures attract administrative fines and naming and shaming of the offending company by the authorities through the National Enterprise Credit Information Publicity System.

Conclusion

The Measures aim to reduce false and misleading advertisings, and provide certainty to advertisers as to their obligations and responsibilities when promoting pharmaceutical products.

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

Be Careful What You Draft For – Hong Kong Court of First Instance Clarifies Interpretation of Arbitration Clauses

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

As more companies seek to resolve intellectual property disputes through arbitration rather than litigation, it is vital that arbitration clauses are drafted clearly and without ambiguity. Clarity in drafting will minimise the risk of future arguments in case one party changes its mind.

The recent case of *Giorgio Armani SPA & Ors v Elan Clothes Co Ltd* [2019] HKCFI 2983 ("**Judgment**") demonstrates the adverse effect where an arbitration clause leaves too much room for interpretation, and how the court will interpret the clause in such circumstances.

The Facts – What Happened?

In December 2014, Giorgio Armani SPA ("**Armani SPA**") entered into a master agreement ("**MA**") with Elan Clothes Co Ltd ("**Elan**"). The MA authorised Elan to open and operate single brand stores in the PRC selling products using Armani SPA's trade marks. The MA contained an arbitration clause ("**Arbitration Clause**") which provided that any dispute, controversy or claim deriving from, arising out of or regarding

the MA, "including any dispute regarding its validity, interpretation, construction, performance, breach and termination, would be settled by arbitration at the Hong Kong International Arbitration Centre".

The relationship between the parties broke down in 2017, after Armani SPA suddenly announced a rebranding exercise of certain brands, causing Elan substantial losses. Elan ceased paying Armani SPA royalties and other fees due under the MA. In response, Armani SPA served a notice of termination of the MA and initiated arbitral proceedings against Elan in Hong Kong seeking, among other things, a declaration that it legitimately terminated the MA and damages. An arbitral tribunal ("**Tribunal**") was then constituted in Hong Kong.

Notwithstanding the commencement of the arbitration, Elan brought parallel proceedings in Shandong, Mainland China ("**Shandong Proceedings**") against Armani SPA, Giorgio Armani Shanghai, Giorgio Armani Hong Kong and Mr. Giorgio Armani (collectively, "**Armani Affiliates**") for contravening Chinese consumer protection and tort laws due to the rebranding exercise.

In response, Armani SPA and the Armani Affiliates went to the Hong Kong Court of First Instance ("**Court**") and were granted an interim anti-suit injunction banning Elan from continuing the Shandong Proceedings. The final determination of whether a permanent injunction should be granted was dealt with in the Judgment.

The Judgment

The Court considered two issues:

1. Whether the dispute between Elan and Armani SPA and the Armani Affiliates fell within the scope of the Arbitration Clause; and
2. Whether the Court should grant a permanent anti-suit injunction restraining Elan from proceeding with the Shandong Proceedings.

(I) THE SCOPE OF THE ARBITRATION CLAUSE

Armani SPA and the Armani Affiliates contended that Elan's claims in the Shandong Proceedings fell within the scope of the Arbitration Clause. Elan responded that its claims, at least against the Armani Affiliates, were outside the scope of the Arbitration Clause since the only contracting parties to the MA were Armani SPA and Elan.

The Court found that, from an overall review of the MA, the Arbitration Clause was intended to cover not only Armani SPA, but also the Armani Affiliates. Although the Armani Affiliates were not parties to the MA, the Court highlighted that the MA, as a whole, contained multiple references to "Affiliates" and was expressed to be made "by and between" Armani SPA together with its "Affiliates". It followed that the Arbitration Clause was intended to cover disputes arising from the MA which also relate to the Armani Affiliates.

Additionally, the Court cited the *Fiona Trust* principles, which provide that arbitration clauses should be interpreted with reference to the presumption that parties, as rational businessmen, would have intended any disputes arising from their relationship to be decided by the same tribunal, unless very clear wording states otherwise. Since the dispute between Elan and the Armani Affiliates, like the dispute between Elan and Armani SPA, also arose from Armani SPA's rebranding exercise, all such disputes should be adjudicated by one arbitral tribunal pursuant to the Arbitration Clause (i.e. the Tribunal). Accordingly, by instituting the Shandong Proceedings against Armani SPA and the Armani Affiliates, Elan acted in breach of the Arbitration Clause.

(II) WHETHER A PERMANENT ANTI-SUIT INJUNCTION SHOULD BE GRANTED?

Elan argued that, even if its claims were found to be covered by the Arbitration Clause, the Court should not grant an anti-suit injunction as this was an issue which would be ordinarily decided by the Tribunal. The Court should not pre-empt the Tribunal's decision pursuant to section 45(4) of the Arbitration Ordinance.

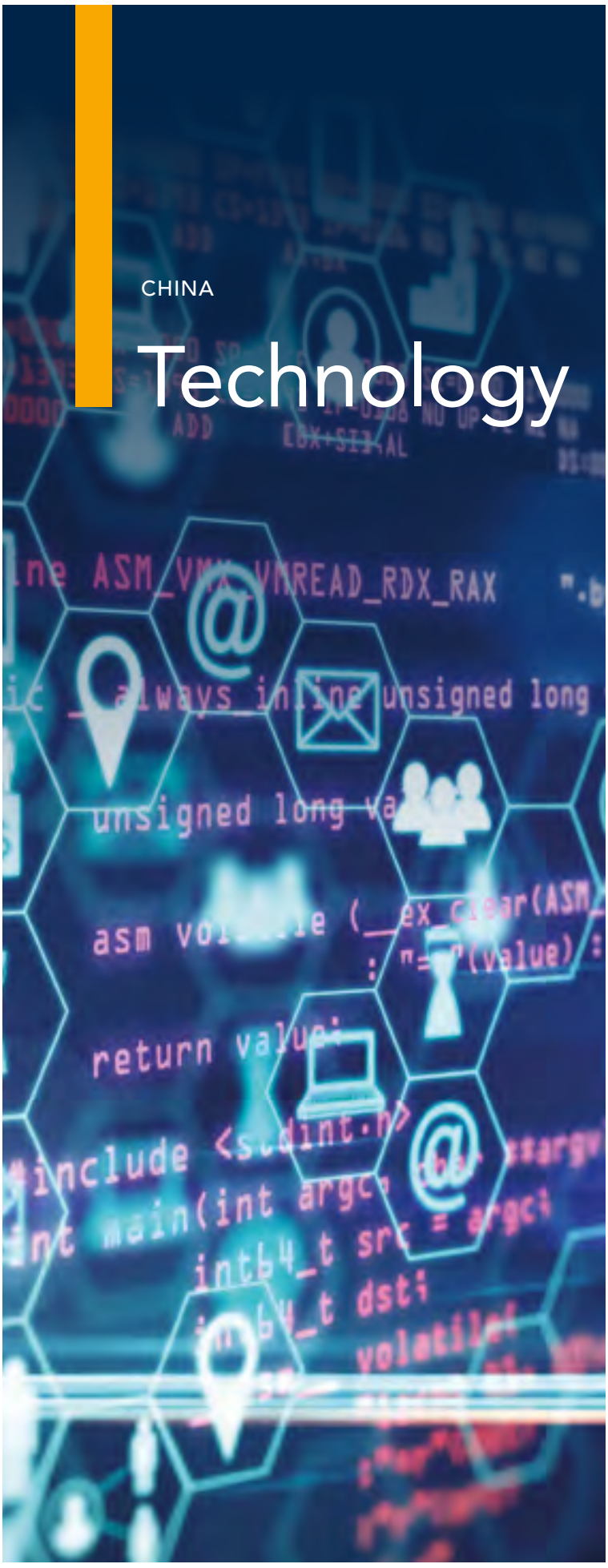
The Court rejected this argument. It first confirmed its jurisdiction to grant an anti-suit injunction to restrain foreign proceedings in breach of an arbitration agreement under section 21L of the High Court Ordinance and/or its inherent jurisdiction. It then held that, even though the anti-suit injunction may overlap with the relief sought by the Plaintiffs in the arbitration, it may still decide to grant the injunction if it is just and convenient to do so. In this connection, the Court found that Elan's act of commencing the Shandong Proceedings was an unreasonable attempt to bypass the Arbitration Clause and to improperly exert pressure on the Armani SPA and the Armani Affiliates. As a result, it

granted a permanent anti-suit injunction to restrain Elan from commencing proceedings otherwise than in accordance with the Arbitration Clause, including the Shandong Proceedings.

Comments

The Judgment is not surprising given the pro-arbitration stance of Hong Kong courts – when parties argue over the ambit of an arbitration clause, courts will likely interpret such a clause widely. Nonetheless, why waste substantial time and costs arguing over the scope of an arbitration clause and commence an anti-suit injunction when the Arbitration Clause should have been drafted more clearly at the outset? This Judgment provides insight as to the importance of drafting arbitration clauses clearly and the potential far-reaching ramifications for not doing so.

*The author would like to thank **Christopher C. H. Ng**, trainee solicitor at Mayer Brown, for his assistance with research for this article.*



Weeding Out Unacceptable Online Content – New Rules in the PRC

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

Cheng Hau Yeo, Associate
Mayer Brown, Singapore

Introduction

On 20 December 2019, the Cyberspace Administration of China released the Regulations on Governance of Online Information Content Ecosystem ("**Regulations**"). The Regulations, which came into force on 1 March 2020, expand on the existing rules regulating online content in China's Cybersecurity Law, National Security Law and the Administrative Measures for Internet Information Services. The main purpose of the Regulations is to build a "positive and healthy" network ecosystem and impose additional obligations on online content producers ("**Content Producers**"), Internet service providers ("**ISPs**") and Internet users.

Background

A day before the Regulations were enacted, the award-winning fanfiction site *Archive of our Own* suddenly became inaccessible in China. There was speculation that this was due to the content posted on the site, dealing mainly with issues of interest to the gay community which were based on the television show *The Untamed* which was in turn based on a gay romance novel. Some had speculated that the ban resulted from complaints to Chinese authorities over the

"lewd" nature of the gay romance featured on the site. Whatever the cause of the Regulations, it is clear that their enactment signals a shift towards active policing, with the responsibility to review and sift out inappropriate online content now falling on ISPs as well and not just on websites owners.

Key Aspects of the Regulations

The Regulations stipulate that content posted online should be positive, uplifting in nature, and based on fact and not rumour. Content deemed unacceptable include the usual panoply of content harming "national honour and interests, spreading rumours, disrupting social order, embodying sexual innuendos, horror, brutality, vulgarity, and inappropriate commentary on natural disasters and major accidents". Notably, the Regulations impose more onerous obligations on ISPs which will require them to apply significant modifications to their online review mechanisms. Below are some provisions in the Regulations that may be of particular interest to organisations which host or create website content in China.

(I) CONTENT PRODUCERS: DELINEATING "GOOD" AND "BAD" ONLINE CONTENT

The Regulations set out content that is encouraged, content that is classified as "illegal" and content that if possible should not be published. These different shades of grey are set out below. The content that Content Producers are encouraged to publish, includes content that:

i. Highlights the nation's economic and social development, which reflects the people's great struggle and enthusiastic life spirit;
ii. Responds to social concerns, dispels doubts and clarifies facts to help the general public reach a consensus;
iii. Contributes to enhancing the international influence of Chinese culture and presents a realistic, three-dimensional China to the world; and
iv. Promotes taste, style and responsibility, compliments truth, goodness and beauty, and encourages unity and stability

A blanket ban is imposed on a list of content that is classified as "illegal content", such as content that:

i. Spreads rumours to disturb economic and social order;
ii. Jeopardises national security and undermines national unity;
iii. Damages the reputation or interests of the state;
iv. Distorts and defames the deeds and spirits of national heroes and martyrs; and
v. Undermines ethnic unity or encourages ethnic animosity or discrimination.

It is worth noting that some of the categories of banned content (e.g. content that defames national heroes and martyrs) were not previously prohibited by the Chinese government.

The content that Content Producers are required to take measures to prevent and resist publishing, includes content that:

i. Has exaggerated titles that are patently inconsistent with the content;
ii. Contains gossips or scandalous material that may cause public hype;
iii. Contains improper comments on disasters (natural or otherwise);
iv. Contains sexual innuendos or provocations; and
v. Otherwise has an adverse effect on the online ecosystem (this is notably a catch-all provision).

These new categories of content reveal the tight grip that the Regulations impose over online content. In particular, it is no longer sufficient to simply remove negative content after it has been published. With the Regulations stipulating that Content Producers must also actively *prevent* such content from being published, it appears that a more stringent standard has been imposed and therefore more active policing will be required.

(II) ISPS: MORE ONEROUS OBLIGATIONS

ISPs must put in place mechanisms for governing the online content ecosystem. Examples of such mechanisms include actively managing user accounts, assessing comments and information for publication, conducting real-time inspections and designating a person in charge for governing online content.

ISPs are also required to actively display "positive" content in the form of links on home pages and pop-ups of websites, and default Internet searches. In addition, ISPs must conduct enhanced inspections of advertisements on their websites, establish

convenient channels for filing complaints in prominent places and compile an annual report on the measures they have taken to regulate network information content. ISPs should be mindful of the consequences of non-compliance, which may entail both civil and criminal liability. Notably, the Regulations stipulate that non-compliance will be dealt with by cyberspace authorities and relevant departments in conjunction with existing laws, such as the Cybersecurity Law and the Administrative Measures for Internet Information Services. In short, ISPs should be aware of any overlapping obligations and ensure that they comply with the new Regulations as well as other applicable laws.

Takeaways

With the enactment of the Regulations, organisations which provide, publish or host content should have a heightened awareness of "good" and "bad" content to avoid violating the Regulations. Content Producers, ISPs and Internet users are now expected to actively police content published online. ISPs have also become subject to more stringent requirements. The Regulations should be read in conjunction with the existing Cybersecurity Law and organisations should review their existing measures relating to content publishing and policing and update them where necessary to comply with the new Regulations. The extra-territorial effect of the Regulations is unclear for now but the increasing global popularity of Chinese-run social media apps such as TikTok, will no doubt test this.

Contact Us

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

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

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

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