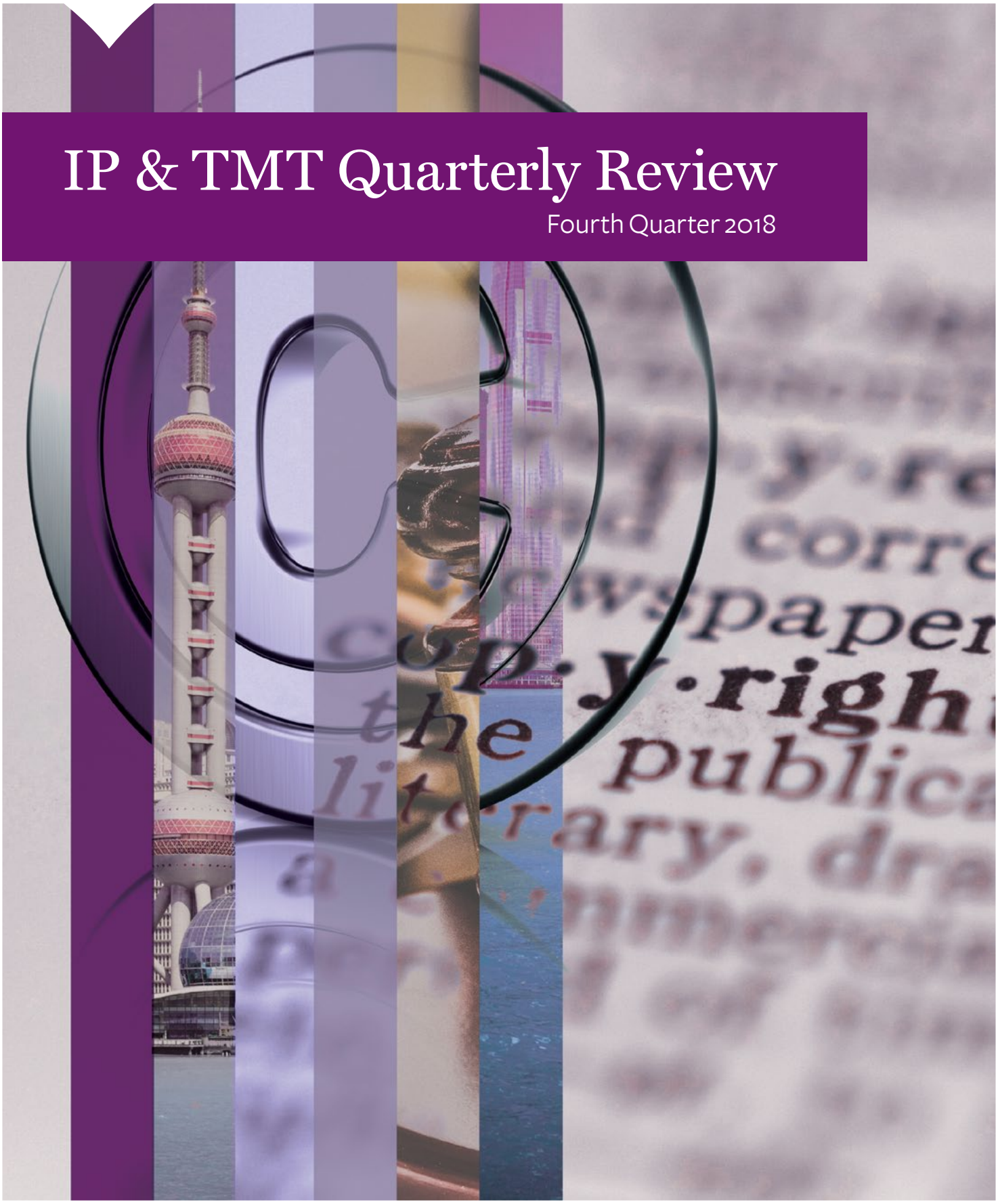
MAYER·BROWN

IP & TMT Quarterly Review

Fourth Quarter 2018

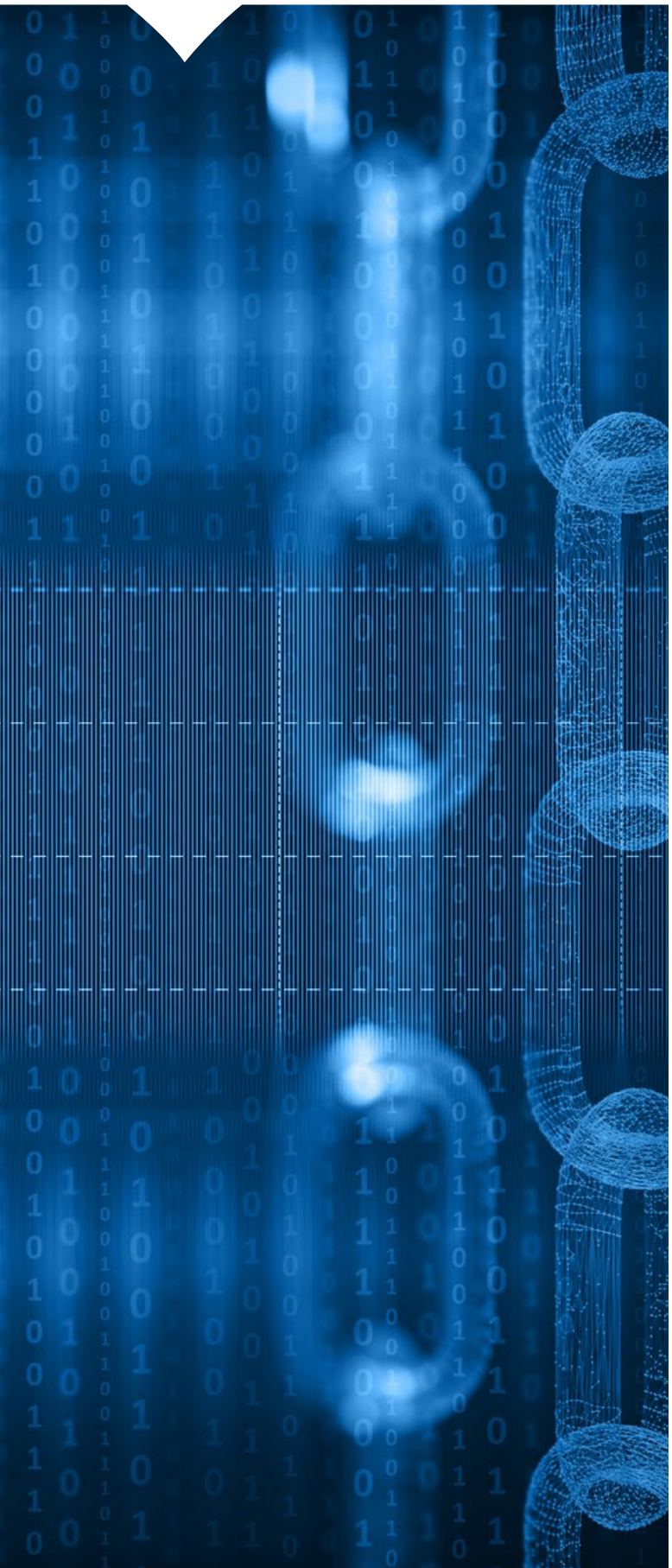


Contents

Key: Click to Navigate

Intellectual Property

By Gabriela Kennedy, Partner, Mayer Brown, Hong Kong
Rosana She, Registered Foreign Lawyer, Mayer Brown, Hong Kong



IP Courts: Ringing in the Changes

Specialist Appellate Intellectual Property Tribunal in China

On 26 October 2018, in the *Decision of the Standing Committee of the National People's Congress on Several Issues concerning Judicial Procedures for Patent and Other Intellectual Property Cases* ("**Decision**"), the National People's Congress Standing Committee ("**NPCSC**") of China confirmed its plan to set up an appellate Intellectual Property tribunal ("**IP Tribunal**") within the Supreme People's Court ("**SPC**"). This Decision will become effective on 1 January 2019, which means the SPC, via the IP Tribunal, will have jurisdiction to hear appeals of first instance judgments from 1 January 2019. The SPC is required to report to NPCSC on the progress and performance of the IP Tribunal in January 2022.[1]

The aim of the Decision is to create a unified ruling standard for IP litigation in China to achieve the following: further strengthen the legal protection of IP rights, enhance the legal enforcement environment for technological innovation and advance the implementation of innovation-driven development strategies.[2]

Further Developing the IP Specialist Courts System

Back in August 2014 the NPCSC passed a decision to establish IP specialist courts in Beijing, Shanghai and Guangzhou to hear IP disputes.[3] In 2017, IP specialist court rooms were set up in 15 cities, including Hangzhou, Nanjing and Suzhou. These IP courts and court rooms (collectively, "**IP Courts**") determine IP cases at the first instance. Under the current system, first instance administrative and civil cases related to

1 Article 4 of the Decision.
2 Preamble of the Decision.
3 *Decision of the Standing Committee of the National People's Congress on Establishing Intellectual Property Courts in Beijing, Shanghai and Guangzhou* ("**Decision on Establishing IP Courts**").

patents are under the jurisdiction of Intermediate People's Courts. Appeals of such cases are heard at the Higher People's Courts located in the region of the relevant IP Courts.

Under the new IP appellate system, the IP Tribunal will hear appeals from the IP Courts where the subject of dispute concerns the following IP matters: invention or utility model patents, plant breeders' rights, integrated circuit layout designs, trade secrets, computer software, or antitrust matters.[4] The local Higher People's Courts will no longer have jurisdiction over such appeals. The IP Tribunal will also have the power to order the relevant lower courts to re-try these cases. Appeals of other first-instance cases that are unrelated to IP matters mentioned above will continue to be tried at the relevant local Higher People's Courts.

Potentially Higher Degree of Certainty in Judicial Interpretation

The SPC recognises that the areas of IP involved in the IP Tribunal appeals are very specialised and require knowledge in the relevant areas for the purpose of determining a case. If the judges appointed to the IP Tribunal have the relevant expertise, and are willing to consult relevant subject matter experts in reaching a decision, useful reference cases may potentially emerge and help companies navigate the IP enforcement landscape in China.

But What about Hong Kong?

To date, no specialist court, list or judge are available in Hong Kong to hear IP cases. At present, any IP actions are to be filed in the general list at the Court of First Instance of the High Court. After years of discussion in the legal community, the Hong Kong Judiciary appears to be finally answering the calls for the establishment of a specialist IP court or list, and appointing specialist IP judges, to hear IP cases in Hong Kong. Though no official announcement has been made by the Hong Kong Judiciary, in early December 2018 at the Business of IP Asia Forum, Mr Justice David Lok of the Court of First Instance of the High Court discussed proposed changes with respect to IP litigation, including the potential establishment of a new specialist IP list in the High Court in 2019.[5]

While Hong Kong seeks to develop a knowledge-based economy, the technology and R&D sectors in Hong Kong are still relatively young. An IP list in the High Court is to be welcomed, but its success will depend on the specialist skills that will have to be deployed to guarantee its efficiency

Internet Courts in China

In September 2018, the Supreme People's Court of China ("**SPC**") issued the "Provisions of the Supreme People's Court on Several Issues concerning the Trial of Cases by Internet Courts" ("**Provisions**"). The Provisions provide useful guidance for online trial procedures at Internet Courts in China.

Rising Popularity of Pilot Hangzhou Internet Court

The first Internet Court was inaugurated in August 2017 in Hangzhou, the city that is sometimes dubbed China's "Silicon Valley"[6], which is of course home to Alibaba, one of China's e-commerce giants. As at August 2018, the Hangzhou Internet Court has heard over 12,000 cases and concluded over 10,000 cases. The average duration of a case at the Hangzhou Internet Court is only 41 days, which amounts to a time saving of approximately 50% compared to litigating at a traditional court in China.[7]

4 Articles 1 and 2 of the Decision on Establishing IP Courts.

5 Mr Justice David Lok, "*The Proposed Changes in the Conduct of IP Litigation in the High Court of Hong Kong*", Business of IP Asia Forum, HKSAR Government, Hong Kong Trade Development Council and Hong Kong Design Centre, December 7 2018.

6 Maggie Zhang, Hangzhou, "*China's answer to Silicon Valley, is a hit with returning graduates, study finds*", South China Morning Post, 2 July 2018, https://www.scmp.com/business/companies/article/2152935/hangzhou-chinas-answer-silicon-valley-hit-returning-graduates.

7 Please refer to an article published in Chinese by the Office of the Central Cyberspace Affairs Commission with the translated title "H*ow to run an online trial – reporter visits the Beijing Internet Court*" at: http://www.cac.gov.cn/2018-09/10/c_1123404946.htm.

Intellectual Property Cont'd

Online Trials: Keeping up with the Times

The Hangzhou Internet Court also sanctioned the use of blockchain as evidence in judicial proceedings in a copyright infringement dispute.[8] Given that the Hangzhou Internet Court is a lower court that hears cases at first instance only, the Provisions provide a welcome confirmation in relation to the admissibility of blockchain evidence in judicial proceedings in China. Article 11 of the Provisions specifies that if a litigant can prove the authenticity of any evidence involving digital data by, for example, using blockchain, digital timestamp and electronic signature, the Internet Courts will accept such evidence. The other party can also apply for submission to the Internet Courts for reports to be prepared by experts with specialist digital data knowledge to contest the reliability of such evidence. It seems that for now the courts in China are leading the way with regard to the acceptance of new technologies to support the provision of evidence.

Internet Courts: Geographic Expansion and Expanded Case Coverage

In addition to confirming the applicability of blockchain, the Provisions specify the jurisdiction of Internet Courts, and trial and appeal procedures relevant to online trials. The Provisions will be useful guidelines for the Hangzhou Internet Court going forward, as well as for the Beijing and Guangzhou Internet Courts, which were set up in early and late September 2018 respectively. Each of the two additional Internet Courts heard their first cases in October 2018, with plenty more to follow. As at late October 2018, almost 5,500 cases had been received by the Beijing Internet Court[9], while the Guangzhou Internet Court had received over 1,100 cases[10].

The Provisions confirm that the three Internet Courts can hear cases at first instance that involve disputes regarding: e-commerce terms of service; service agreements that are executed online; loans executed online; copyright and neighbouring rights; domain names; and product liability in relation to defective products purchased online. They also have jurisdiction over internet-related public interest litigation brought by public prosecutors, and other internet-related civil or administrative cases assigned by a higher court.[11]

The new Internet Courts also have jurisdiction over domain name disputes. Given the two-year limitation period for .cn DRP disputes, and the fact that Internet Courts deal with cases in a comparable time-frame to that of .cn cases brought under the .cn DRP, we expect to see them become a popular forum for .cn disputes, especially in cases outside the two-year limitation period.

The Future of IP and Technology Disputes may be Online

The success of the Hangzhou Internet Court so far, both in terms of efficiency and the embrace of technology in trial proceedings, and the prevalence of e-transactions in China coupled with the setting up of two new Internet Courts in China signals a new era for dispute resolution underpinned by an open-minded approach when it comes to using new technology to accept evidence and deliver decisions. ◆

8 Please refer to a report on the case published in Chinese on People.cn with the translated title "*Copyright dispute - Blockchain as 'witness'*" at: http://ip.people.com.cn/BIG5/n1/2018/0724/c179663-30165424.html.

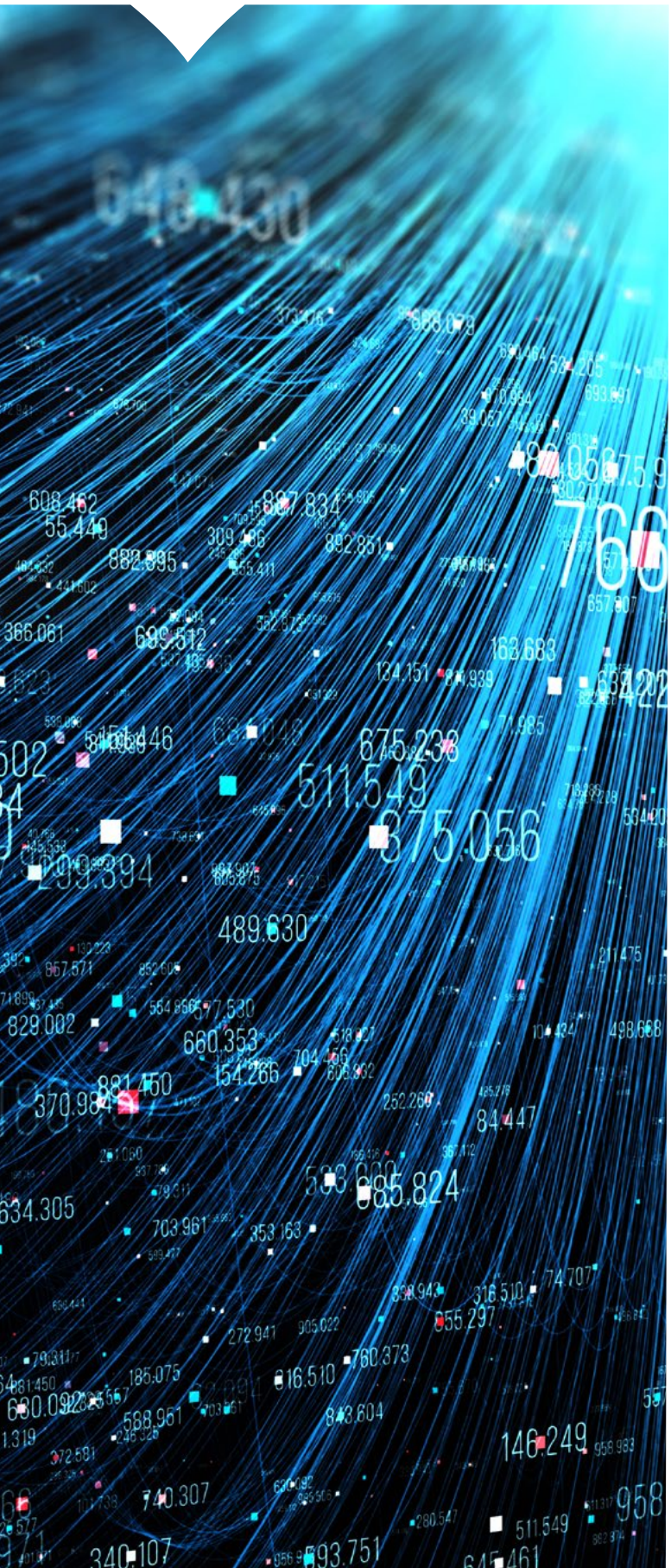
9 Please refer to an article published in Chinese by Xinhua News at: http://www.xinhuanet.com/legal/2018-10/31/c_1123637834.htm.

10 Please refer to an article published in Chinese by the Office of the Central Cyberspace Affairs Commission with the translated title "*Guangzhou Internet Court delivers first decision – Litigants attends online court*" at: http://www.cac.gov.cn/2018-10/31/c_1123636937.htm.

11 Article 2 of the Provisions.

Intellectual Property

By Benjamin Choi, Partner, Mayer Brown, Hong Kong
Vivian Or, Senior Associate, Mayer Brown, Hong Kong



Time for a Change: Updates in Technology to Assist with Trade Mark Searches and Registrations

As discussed in the Q3 2018 issue of our IP & TMT Quarterly Review, the Hong Kong Trade Marks (Amendment) Bill 2018 ("**Bill**") intends to introduce new provisions in light of Hong Kong acceding to the Protocol Relating to the Madrid Agreement Concerning the International Registration of Marks ("**Madrid Protocol**")[12]. With updates to the trade mark law and registration procedure in Hong Kong becoming imminent, there is also a pressing need for the Hong Kong Intellectual Property Department ("**IPD**") to upgrade its IT system in order to better facilitate its integration with the World Intellectual Property Organization ("**WIPO**")'s Madrid System.

To this effect, the IPD has commissioned the development of a New Integrated IT System ("**NIS**"). It is expected that the NIS will be deployed and commence operations in February 2019.

Hong Kong is not the only one giving a "face lift" to its IT systems. On 27 November 2018, the PRC State Intellectual Property Office ("**SIPO**") introduced a new online trade mark service system ("**SIPO's New Service System**") to provide an updated and efficient platform for the public to search for trade mark-related documents.

NIS and Workshops by IPD

The launch of the NIS will help streamline the process of e-filing and e-searches for trade marks, designs and patents. It will enable trade mark searches to reveal an unlimited number of records, as opposed to the current search results, which can only show up to 1,000 records. This means that users will no longer need to

12 Please refer to our Asia IP & TMT Quarterly Review 2018 Q3 for further discussion on the Trade Marks (Amendment) Bill 2018 and the Madrid Protocol at https://www.mayerbrown.com/files/Publication/8b32a036-3c99-40e1-8fba-6798a8159eab/Presentation/PublicationAttachment/12b6cead-e1c2-4078-a9b2-7e7ec85bbe01/ASI-IP-TMT-QuarterlyReview-2018Q3.pdf.

Intellectual Property Cont'd

restrict search criteria to generate statistics accurately and efficiently. The NIS will also introduce a new business-to-business e-filing capability that will enable bulk filings of applications and renewals of registrations in a single online process.

The IPD does not intend to run the old and new IT systems in parallel for a transitional period: the NIS will immediately replace the current system upon its launch. To prepare for the upcoming roll out and to enable easy assimilation of the NIS, the IPD offered workshops, such as the Focus User Group Meeting B2B (system to system) e-Filing service, and carried out User Acceptance Tests ("**UAT**"), in October 2018. Participants in the UAT workshops had a first-hand experience in navigating through the NIS, and the IPD has been busy fixing any bugs and issues identified during the UAT.

Due to the implementation of the NIS, the following services will be affected:

a. E-filing service: the service will be suspended for about 10 days. During this period, the IPD will only receive forms and correspondences at the Public Service Counter or by mail, subject to the extended opening hours of the IPD;
b. Online search service: the online search service will still be available but the accuracy of the data will be affected (i.e. showing data prior to the suspension period); and
c. Official journal: the publication of the official journal will be suspended for two weeks for the acceptance of trade marks, five weeks for request to record or for grant of patents and four weeks for the registration of designs. Other notices published under the Trade Marks Ordinance (Cap. 559), Patents Ordinance (Cap. 514) and Registered Designs Ordinance (Cap. 522) will be suspended for two weeks.

SIPO's New Service System and SIPO's Future Plan

The PRC has also been busy by launching the SIPO's New Service System in November 2018, which provides an updated, transparent and efficient platform for the public to search for trade mark-related documents. The public can now quickly retrieve documents such as certificates of registration and priority documents with just the trade mark registration number or the registrant's name.

In light of the current increasing trend of using QR codes, the SIPO has also decided to incorporate QR codes on the trade mark registration certificates. This will enable the public to scan the QR code on a certificate, which would lead them to the SIPO's New Service System to help verify the certificate's content, validity and authenticity.

Conclusion

Given the rapid pace of development of technology and the growing demand for efficient solutions, the IPD's NIS and the SIPO's New Service System are to be welcomed. The system upgrades will enable the public to obtain and verify IP information online more quickly and efficiently. ◆

HONG KONG

Advertising

By Gabriela Kennedy, Partner, Mayer Brown, Hong Kong
Amita Haylock, Counsel, Mayer Brown, Hong Kong

Compare, but Beware – Recent Judgment on Comparative Advertising in Hong Kong

Introduction

Historically, there have always been tensions in intellectual property law around how to balance the exclusive rights granted to intellectual property rights owners, while also allow for healthy competition between businesses to benefit consumers. One area where this tension is evident is in comparative advertising – e.g. where advertising materials identify a competitor, and identify a company's products or services as superior.

A recent judgment of the Hong Kong High Court ("**Court**") provides guidance on comparative advertising for the first time, including the interpretation of section 21 of the Trade Mark Ordinance (Cap. 559) ("**TMO**")[13]. In this case, the Court dismissed a trade mark infringement claim brought by the PCCW-HKT Group ("**PCCW**"), against its competitor, Hong Kong Broadband Network Limited ("**HKBN**")[14]. In doing so, the Court demonstrated support for comparative advertising, allowing more freedom for advertisers to highlight their companies' market advantages, and encouraging healthy competition.

Background

In 2015, HKBN launched an advertising campaign with a number of catchphrases that included: "*PCCW Home Telephone Service customers say goodbye to bloated monthly fees!*" and "*電訊盈科家居電話用戶唔駛再忍受咁大食嘅家居電話用費*". These catchphrases included trade marks registered by PCCW, such as "PCCW" and "電訊盈科" ("**Marks**").

13 Section 21 of the TMO deals with a defence to trade mark infringement where there would be no infringement of registered trade marks, if they are used in accordance with honest practices in industrial or commercial matters.

14 *PCCW-HKT Datacom v Hong Kong Broadband Network Limited* [2018] HKCFI 2037.

Advertising Cont'd

There was no dispute by the parties that HKBN used the Marks. However, PCCW argued that HKBN had infringed PCCW's trade mark rights under sections 18(1) and (4) of TMO, as HKBN used the Marks in the course of business, thus taking unfair advantage of the reputation of the Marks. HKBN relied on section 21 of the TMO as a defence which states that there is no infringement of registered trade marks, if they are used in accordance with honest practices in industrial or commercial matters.

The factors that the Court may consider in determining "honest practices" include, in particular, whether:

a. the use takes unfair advantage of the trade mark;
b. the use is detrimental to the distinctive character or repute of the trade mark; or
c. the use is such as to deceive the public.

PCCW claimed that HKBN's use of the Marks was not in accordance with honest practices in industrial or commercial matters. One of the reasons given to support this contention was the use in the advertisements of the expressions "*bloated fees*" and "大食" (meaning gluttonous in Chinese).

HKBN rebutted this claim by asserting that a reasonable consumer reading the advertisements would likely take the view that the catchphrases used were honest[15], true and not misleading, and that the use of "*bloated*" and "大食" (i.e. gluttonous) was just advertising language or puff, with no effect of discrediting PCCW, given the context of the advertisements.

Judgment

The Court held that HKBN had successfully established a defence under section 21 of the TMO against PCCW's infringement claim, as the use of the Marks was in accordance with honest practices in industrial or commercial matters.

The Court also held that the purpose of comparative advertising is to identify the differences of services between competitors. Here, HKBN did not seek to use the Marks to benefit from their attributes or take a "free-ride", but was merely highlighting the price differences between the parties. Hence, there was no unfair advantage taken of the Marks.

In determining the meaning of "honest practices", the judge took into consideration the test of whether a reasonable man would take the claim in the advertisement to be one which was made seriously.[16] The judge held that an average consumer in Hong Kong would be used to price comparisons of services, and would understand the words "*bloated*" and "大食" (i.e. gluttonous) as merely meaning "expensive" in more colourful language. Therefore, there was nothing unfair or dishonest when HKBN highlighted their reduced prices using the Marks and the expressions.

Other Jurisdictions

Comparative advertising is not explicitly prohibited under the Advertising Law of the People's Republic of China ("**PRC**")[17], however, advertisements should not disparage ("贬低") the goods or services of any other producer or trader (Article 13) and should not engage in any form of unfair competition (Article 31).

While both Hong Kong and the PRC have not made direct references to the use of comparative advertising in their trade marks and/or advertising legislations, some jurisdictions in Asia-Pacific, such as Australia and Singapore have. The Australian Trade Marks Act exempts trade mark infringement in the context of comparative advertising.[18] According to Australian case law, while there are no special principles that apply

15 Evidence was adduced to show that during the relevant period, PCCW's prices for fixed line telephone service were "largely" more expensive than HKBN.
16 A test established in the English case: *Vodafone Group PLC v Orange Personal Communications Services Ltd* [1997] FSR 34.
17 Please refer to the Advertising Law of the PRC at: http://www.npc.gov.cn/npc/cwhhy/12jcwh/2015-04/25/content_1934594.htm (Chinese only).
18 Section 122(1)(d): "... a person does not infringe a registered trade mark when... the person uses the trade mark for the purposes of comparative advertising".

to comparative advertising, the facts in the advertisements must be true and accurate.[19] As for Singapore, the Singaporean Trade Marks Act explicitly caters for the "*fair use*" of a registered trade mark in comparative advertising.[20] One of the factors which the court will take into account when interpreting "*fair use*" is whether the average consumer would find the advertisement materially misleading.[21]

Both Hong Kong and the PRC have legislations to prevent the use of misleading information in advertisements. Under the Trade Description Ordinance (Cap. 362), any person who applies a false trade description (defined to include a misleading trade description[22]) in an advertisement in the course of trade or business, commits an offence.[23] Similarly, under Article 8 of the Anti-Unfair Competition Law of the PRC, business operators may not promote their goods or services in a false or misleading manner, in an attempt to defraud or mislead consumers.[24]

Conclusion

In the recent PCCW/HKBN judgment, the Court's interpretation of the provision governing the use of a trade mark in advertising in Hong Kong demonstrates a support for comparative advertising, whilst also clarifying the test to be applied for a party to rely on the provision.

In a city that is unapologetically focused on a free market economy, business in Hong Kong is highly competitive. The support for comparative advertising aligns with Hong Kong's *laissez-faire* ideology. This should encourage fair competition, and also enable businesses to cater their goods or services to meet consumer demands and expectations. ◆

19 *Gillette Australia Pty Ltd v Energizer Australia Pty Ltd* [2002] FCAFC 223.

20 Section 28(4)(a): "... a person who uses a registered trade mark does not infringe the trade mark if such use... constitutes fair use in comparative commercial advertising or promotion".

21 *Allergan Inc. & Anor v Ferlandz Nutra Pte Ltd* [2016] SGHC 131.

22 Section 2 of the Trade Description Ordinance.

23 Section 7(1) of the Trade Description Ordinance: "... any person who – in the course of any trade or business— (i) applies a false trade description to any goods; or (ii) supplies or offers to supply any goods to which a false trade description is applied... commits an offence".

Section 8(1) of the Trade Description Ordinance: "The following provisions of this section shall have effect where in an advertisement a trade description is used in relation to any class of goods or services."

Section 8(2) of the Trade Description Ordinance: "The trade description is to be taken as referring to all goods or services... for the purpose of determining whether an offence has been committed under section 7(1)(a)(i)".

24 Please refer to the Anti-Unfair Competition Law of the PRC at: http://www.npc.gov.cn/npc/xinwen/2017-11/04/content_2031432.htm (Chinese only).

HONG KONG

Data Privacy

By Gabriela Kennedy, Partner, Mayer Brown, Hong Kong
Karen H. F. Lee, Senior Associate, Mayer Brown, Hong Kong

Change it Up: Amendments to the Hong Kong Personal Data (Privacy) Ordinance Being Considered

Recent high profile data privacy breaches have brought the Hong Kong Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**") under the spotlight. Hong Kong was one of the first countries in Asia to enact a data privacy law, and was considered ahead of its time (the PDPO came into operation in 1996). However, the world has caught up, and Hong Kong is now in danger of falling behind.

Over the last couple of years we have seen various countries updating their data privacy laws to keep abreast of changes in technology, as well as changes in the expectations of the public as to their data privacy rights. Japan amended the Act on the Protection of Personal Information which came into force in 2017; China's new Cybersecurity Law came into effect in June 2017; Australia introduced a mandatory data breach notification scheme on 22 February 2018; the EU General Data Protection Regulation ("**GDPR**") that came into force on 25 May 2018; Vietnam passed a new Cybersecurity Law that will came into operation on 1 January 2019; and Thailand's Personal Data Protection Bill is expected to be enacted in the near future.

Shortcomings of the PDPO?

The Hong Kong's Privacy Commissioner for Personal Data ("**PCPD**") has a statutory obligation to review the PDPO from time to time. The PCPD's last review resulted in the 2012 amendments, the major change of which was the introduction of direct marketing restrictions. New concerns have arisen on the potential inadequacies of the PDPO. In particular, the absence of a mandatory data breach notification system, inadequate penalties for failing to comply with the PDPO, the lack of regulation of data processors, and the lack of cross-border transfer restrictions. This has resulted in the PCPD announcing that he will carry out a review of the PDPO in order to recommend potential changes.

DATA BREACH NOTIFICATION

There is currently no provision in the PDPO obliging data users to notify affected data subjects or the PCPD of any data beach, no matter what the scope or potential impact of the breach is. Whilst notification is strongly recommended by the PCPD, no direct sanctions are imposed on data users for failing to do so.

In contrast, the GDPR requires data controllers to report any data breach within 72 hours of it being discovered if the breach is likely to result in any risk to an individual's rights or freedoms. This obligation does not just rest with the data controllers, but also data processors who are obligated to promptly notify their customers and relevant data controllers. South Korea also imposes a mandatory data breach notification, as well as Australia, which requires a notification to be made if the breach is likely to result in serious harm to any affected individuals.

The reporting of all data breaches (no matter how minor) would be impractical. However, taking a page from the GDPR and the new provisions in Australia, an obligation to notify affected data subjects and the PCPD of any data breaches that meet a certain threshold (e.g. a breach that could result in harm to the data subjects), would be a reasonable change to the PDPO. Considering the upheaval and criticisms voiced by the public in the wake of recent data breaches, such a notification requirement would be on a par with what the public already expects.

SANCTIONS

The slew of data breaches over the last year has raised concerns that the sanctions imposed on data users are insufficient. A breach of any of the data protection principles under the PDPO (e.g. failure to implement adequate security measures to protect the personal data, etc.) does not in itself constitute an offence or result in any penalties. Instead, the PCPD has the power to issue an enforcement notice requiring the data user to take steps to rectify or prevent the recurrence of the breach. It is only if a data user fails to comply with the enforcement notice, or commits a new breach on the same facts, that such will amount to an offence. Even then, the maximum fine that can be imposed is only HK$ 50,000 and 2 years imprisonment (plus a daily fine of HK$ 1,000 if the offence continues). If a data user has breached more than one enforcement notice, then the maximum fine goes up to HK$ 500,000 and 3 years imprisonment. The situation is slightly different in relation to the direct marketing restrictions, the breach of which constitutes a direct offence and can incur a maximum fine of up to HK$ 1,000,000 and 5 years imprisonment.

In comparison, the GDPR imposes fines of up to 4% of the annual global turnover of a data controller or EUR 20 million, whichever is higher. The difference in sanctions between the GDPR and PDPO is overwhelmingly apparent, and explains why organisations all over the world were scrambling to ensure compliance prior to the GDPR taking effect. The PDPO lacks the teeth that would ensure more widespread compliance. For now, the greatest threat to data users is damage to their reputation rather than any financial penalty.

DATA PROCESSORS

Only data users (i.e. those who control the collection, use and processing of personal data) are held ultimately responsible to the PCPD and data subjects for any breach of the PDPO, but not their data processors. Given that a large amount of data breaches are linked to data processors, having some statutory sanctions for data processors makes sense, rather than having data users simply rely on their contractual arrangements with data processors to be able to recover any losses they may suffer.

Unlike the PDPO, the GDPR imposes direct obligations on data processors, who are now accountable to the regulators and data subjects for any breaches. These obligations include keeping a record of their processing activities, implementing security measures, appointing a data protection officer, only processing personal data in accordance with the documented instructions of the relevant data controller, and so on. Data subjects even have the right to bring an action directly against a data processor to recover damages suffered due to the data processor's breach of the GDPR.

Data Privacy Cont'd

As data users can only assert a limited amount of control over their data processors (in terms of contractual obligations), it is reasonable to expect data processors to be held equally accountable for any failure to comply with the PDPO, and to not place the burden of compliance solely on the data users' shoulders. Often data breaches arise at the data processor level, and trying to obtain their cooperation with rectifying or mitigating a breach can be difficult. At present, data users need to rely on ensuring that they have robust contracts in place so that they can hold data processors liable for any breaches and secure their assistance.

CROSS-BORDER TRANSFERS

Hong Kong has the distinction of being one of the first jurisdiction in Asia to adopt a data privacy regime, but also one that has not brought into force provisions dealing specifically with cross-border data transfers. Section 33 of the PDPO ("**Section 33**"), which deals with cross-border data transfers, has never been brought into operation since its enactment in 1995. The only requirements currently in effect are the general notification and consent requirements under the PDPO, which apply equally to the use and transfer of personal data whether inside or outside of Hong Kong. There have been many discussions in the past by the PCPD and the government on whether or not to bring Section 33 into effect. So far, little progress has been made save for a non-binding guidance note issued by the PCPD in December 2014 on cross-border transfers[25].

If Section 33 was brought into force as is, then the transfer of personal data out of Hong Kong would be prohibited, save in the following circumstances:

a. the recipient country is included in a "white list" issued by the PCPD (i.e. jurisdictions that are considered to have laws substantially similar to, or which serve the same purpose as, the PDPO);
b. the data user reasonably believes that the recipient country has laws substantially similar to, or which serve the same purpose as, the PDPO;
c. the data subject has consented to the transfer;
d. the data user has reasonable grounds for believing that the transfer is necessary to avoid or mitigate any adverse action against the data subject, and it is not practicable to obtain the data subject's consent; but if it were practicable, the data subject would provide their consent;
e. the personal data is subject to an exemption from data protection principle 3 of the PDPO (e.g. prevention or detection of crime, etc.); or
f. the data user has taken all reasonable precautions and exercised due diligence to ensure that the personal data will not be used in a manner inconsistent with the provisions of the PDPO (e.g. data user conducts due diligence on the transferee and enters into a data transfer agreement, etc.).

In light of the approach being taken by other jurisdictions, it is likely that the PCPD would recommend that further changes be made to Section 33 before it is brought into operation. For example, the GDPR has provisions allowing the cross-border transfer of data within a corporate group, if it is pursuant to binding corporate rules that have been approved by the relevant National Data Protection Authority. In addition, the cross-border transfer of personal data may be permitted where model clauses are incorporated in the relevant data transfer agreements, or the transfer is necessary for the performance of a contract between the data subject and data controller.

Implementing cross-border transfer restrictions similar to those under the GDPR, may have the dual effect of protecting the personal data, whilst not imposing a major burden on the operation of a data user's business.

25 Please refer to the PCPD's Guidance on Personal Data Protection in Cross-border Data Transfer at: https://www.pcpd.org.hk//english/resources_centre/publications/files/GN_crossborder_e.pdf.

Conclusion

To ensure that Hong Kong remains competitive and is not seen as a "risky" jurisdiction for hosting data, it is important that our data privacy legislation continues to evolve. The PCPD has stated that in making any recommendations for reform, he will take into account the interests of all stakeholders, any legitimate purpose and pressing need for the change, the need for proportionality, and Hong Kong's situation as well as global developments. He will seek to achieve a balance between protecting the rights of individuals, with the need to ensure a free flow of data and freedom of expression.

The PCPD's recommendations would just be the start – the drafting of any subsequent bill and the legislative procedure may mean that it could take years before any changes in the PDPO will be seen. In fact, the 2012 amendments took three years from the issuance of the consultation document until its final enactment. ◆

CHINA

Cybersecurity

By Gabriela Kennedy, Partner, Mayer Brown, Hong Kong
Karen H. F. Lee, Senior Associate, Mayer Brown, Hong Kong

Close Encounters of the Government-kind: China's New Regulation on Internet Supervision and Inspection

On 1 November 2018, China's new Regulation on Internet Security Supervision and Inspection by Public Security Bureaus ("**Regulation**") came into effect. The Regulation grants broad powers to the Public Security Bureaus ("**PSBs**") to closely scrutinise internet service providers and network users to ensure that they are compliant with their cybersecurity obligations.

Background

China's Cybersecurity Law ("**CSL**"), which came into effect on 1 June 2017, has introduced stringent requirements on network operators and operators of critical information infrastructures in relation to cybersecurity and data protection. This includes an obligation on network operators to provide technical support and assistance to PSBs to help protect national security and investigate crimes; implement technical measures to prevent cyber attacks, unauthorised access, viruses or other actions that may endanger their network's security; implement internal security management systems and operating rules; appoint personnel who will be responsible for maintaining the network operator's cybersecurity; and so on.

The Regulation was established under the CSL and other related legislation, in order to clarify the PSBs' powers to carry out cybersecurity inspections.

Scope

The Regulation grants PSBs the right to inspect any internet service providers or network users who provide any of the following services ("**Providers**"):

a. internet access, data centres, content distribution or domain name services;

b. internet information services;

c. internet access to the public; or

d. other internet services.

The application of the Regulation, in line with other regulations issued under the CSL, is quite broad. The PSBs retain the discretion to determine what would amount to "other internet services". The Regulation therefore has the potential of covering any company that simply operates a website, regardless of their industry or sector.

Inspections

The Regulation states that the inspections and oversight by the PSBs are for the purpose of ensuring a Provider's compliance with the following obligations imposed by the CSL and other related laws:

a. recordal requirements with the PSBs by network-using Providers;

b. implementation of cybersecurity management and operating rules, and appointing personnel responsible for cybersecurity;

c. implementation of technical measures to legally record and store users' registration information and internet access logs;

d. implementation of technical measures to prevent computer viruses, cyber attacks, network intrusions, and so on;

e. in relation to the provision of public information services (e.g. public websites, etc.), implementation of measures to prevent the publication or transmission of information prohibited by laws and administrative regulations;

f. provision of technical support and assistance to PSBs in accordance with the law, in relation to the protection of national security, prevention and investigation of terrorist activities or crimes; and

g. implementation of measures consistent with the cybersecurity multi-level scheme pursuant to laws and administrative regulations.

The PSBs' inspections and oversight can be carried out either on-site at the Provider's premises or remotely. If remote access will be used, then the PSBs must give the Provider advance notice of the time and scope of the inspection. However, how much advance notice needs to be provided is not specified, and a public announcement would be sufficient.

By contrast, no prior notice is required for on-site inspection, and PSBs can exercise any of the following powers:

a. enter business premises, server rooms or work places;

b. require the person in charge of the Provider or the cybersecurity management personnel to provide any explanations on matters that are the subject of the PSBs' oversight or inspection;

c. inspect and take copies of any information related to matters that are the subject of the PSBs' oversight or inspection; or

d. check the operation of the technical measures put in place to maintain network and information security.

If the PSB finds any failure by a Provider to comply with its cybersecurity obligations, then it has the power to issue rectification orders for minor violations, or to issue harsher warnings, fines or order the imprisonment of responsible individuals pursuant to the CSL and China's Anti-Terrorism Law.

Confidential and Proprietary Information

Major concerns have been raised regarding the level of access that PSBs will have to confidential information and trade secrets of a Provider. Furthermore, PSBs have the right to use third party service providers who have the technical capabilities to provide support in order to help the PSBs carry out any on-site or remote inspections ("**TSP**"). In theory, this could mean that competitors of a Provider could be appointed as a TSP, thereby providing the competitor with back-door access to the confidential and proprietary information of the Provider.

Cybersecurity Cont'd

To try and minimise these concerns, the Regulation imposes an obligation on the PSBs and their staff to strictly maintain the confidentiality of all personal information, trade secrets, state secrets and private information which they learn during the course of their inspections and oversight. They are also prohibited from selling, disclosing or illegally providing such information to anyone, and can only use it as necessary for the purposes of protecting network security.

TSPs are also prohibited from disrupting the normal operation of the Provider's network, from stealing any network data, or otherwise illegally obtaining, selling or providing any personal information acquired during the conduct of their services for the PSBs.

Whether or not the above restrictions can or will be actively enforced against the PSBs or TSPs still remains an area of concern for many companies.

Conclusion

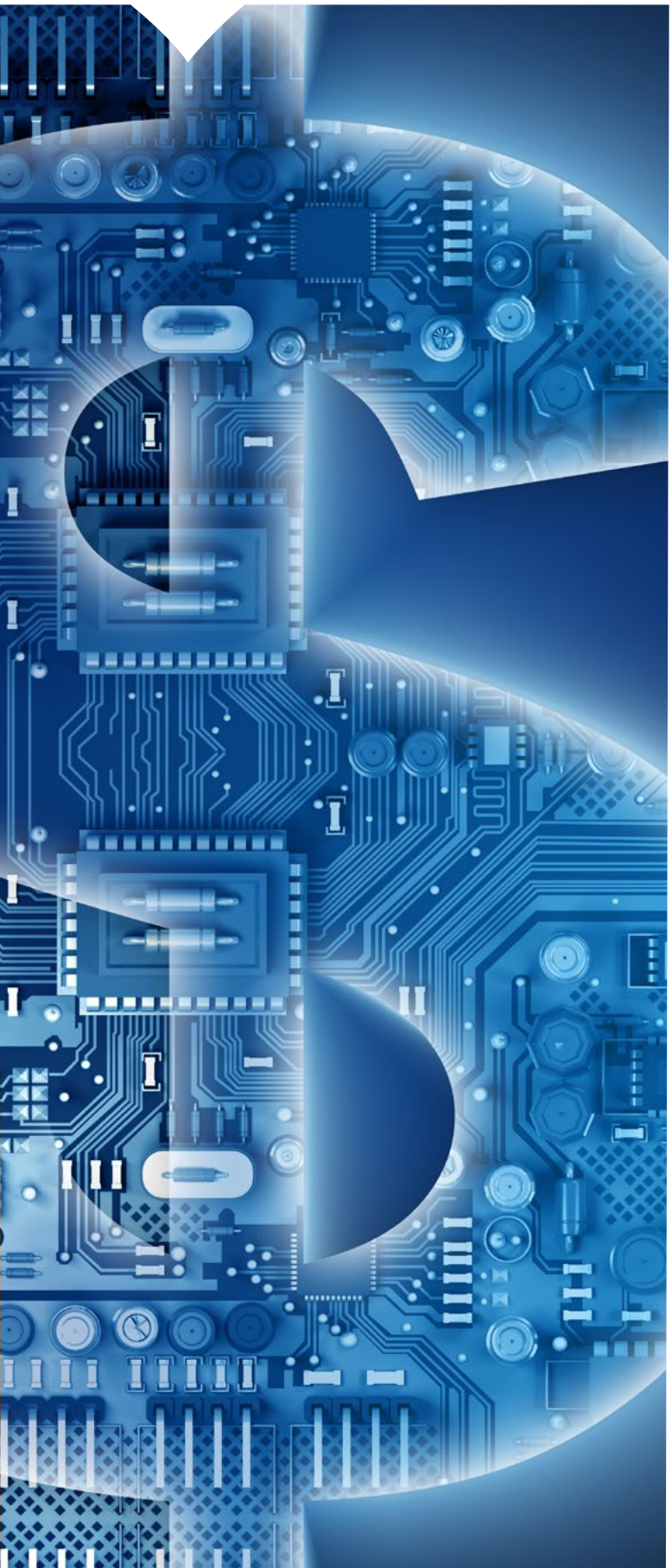
The CSL, amongst other laws and regulations, already grants PSBs with broad powers of scrutiny, which the authorities have already been utilising since the CSL came into force in June 2017. For example, in August 2018, the Ministry of Industry and Information Technology ("**MIIT**") announced that it would be inspecting the networks and systems of organisations in the telecommunication and internet industry to ensure compliance with the CSL. This resulted in MIIT issuing an order on 27 November 2018 against 7 network organisations requiring them to take rectification steps. Some of the deficiencies found by MIIT included a failure to implement cybersecurity management and operating rules, and a failure to carry out cybersecurity emergency drills. What the Regulation does is provide further details on the range of powers available to PSBs. As with the CSL, the Regulation is broad and vague, which unfortunately means a degree of uncertainty on exactly how the PSBs will exercise their powers. Given the amount of ambiguity that still remains with the CSL, and the number of draft measures that have yet to be finalised, companies are left in the tricky position of needing to ensure compliance with the CSL, without knowing the extent of their obligations.

The Regulation cannot be taken as anything but a clear indication that the Chinese authorities are planning on upping their enforcement actions in the coming year. For now, companies operating in China need to take heed of this Regulation, and continue to seek to navigate the unclear path of the CSL to ensure they do not fall foul of their obligations under the main law and/or the complex web of subsidiary regulations. ◆

HONG KONG

Fintech

By Gabriela Kennedy, Partner, Mayer Brown, Hong Kong
Karen H. F. Lee, Senior Associate, Mayer Brown, Hong Kong



Tightening the Reins on Cryptocurrency

On 1 November 2018, Hong Kong's Securities and Futures Commission ("**SFC**") issued a statement and circular that expanded its regulatory reach over virtual asset activities.

Expanding the Scope of the SFC's Supervision

Previously, the SFC's position was that any activities related to virtual assets (e.g. cryptocurrencies, asset-backed tokens, virtual commodities, etc.) would only be subject to the Securities and Futures Ordinance (Cap. 571) if they fell within the definition of "securities" or "futures contracts". However, due to growing concerns over the need to protect investors, the SFC decided to broaden its regulatory oversight to cover all virtual assets, and whether or not they fall within the scope of a "security" or "futures contract". Under the *Statement on Regulatory Framework for Virtual Asset Portfolio Managers, Fund Distributors and Trading Operators* ("**Statement**"), and the *Circular to Intermediaries – Distribution of Virtual Asset Funds* ("**Circular**"), issued on 1 November 2018, asset managers and fund distributors that invest in virtual assets (whether or not they constitute "securities" or "futures contracts") will be subject to the further supervision of the SFC. In particular:

a. any fund managers that solely invest in virtual assets, which do not amount to "securities" or "futures contracts", and who distribute the funds in Hong Kong;

b. any firms that are licensed for Type 9 regulatory activities (asset management) for managing portfolios involving traditional securities and/or futures contracts, who invest (in whole or in part) at least 10% of the gross asset value of their portfolios in virtual assets; and

c. fund distributers that invest solely or partially in virtual assets in Hong Kong.

Fintech Cont'd

In addition, the SFC has decided to establish a conceptual framework to explore the possibility of regulating cryptocurrency exchanges (i.e. virtual asset trading platforms) ("**Platform Operators**") in a "sandbox" environment. Platform Operators can apply to join the SFC Regulatory Sandbox, and the SFC will accept their applications if the Platform Operator can demonstrate that it is committed to complying with the stringent standards expected of it.

During the initial stage, the SFC will consider whether or not it would be appropriate to regulate Platform Operators. The SFC will explain to participating Platform Operators the standards to which they are expected to adhere and will observe their live operations in light of these standards. The SFC will then need to determine, based on its observations, whether the conceptual framework is sufficient and effective to protect investors, and whether Platform Operators are capable of complying with the proposed regulations. If following this initial stage, the SFC finds that it would be appropriate to regulate Platform Operators, then it will consider issuing a Type 1 (dealing in securities) and Type 7 (providing automated trading services) licence to qualified Platform Operators, and impose relevant licensing conditions. Such Platform Operators will then proceed to the next stage of the sandbox for further scrutiny.

For more information regarding the regulatory requirements imposed by the Statement and Circular, please refer to our article entitled *SFC Announcements on Regulatory Approach to Virtual Assets*[26].

Are Regulations Necessary?

The burning question that has arisen in many jurisdictions is whether the cryptocurrency/virtual asset industry needs to be regulated. Can the nature of virtual assets and the related business operations fit into the current regulatory mould imposed by financial authorities? Should it be left up to the industry to self-regulate?

Hong Kong is not the first Asian country to look into regulating cryptocurrency exchanges. A different range of approaches have been applied across the region. With regard to Hong Kong, based on the Statement and Circular, it appears that the SFC is moving towards regulating the cryptocurrency industry as opposed to blocking it. However, some of the regulations proposed by the SFC as part of the conceptual framework, e.g. know-your-customer (or KYC) requirements, may not be conducive to the very nature of the industry, where many transactions are carried out on an anonymous basis.

In China, whilst owning, buying or selling cryptocurrencies is not in itself prohibited, the authorities have cracked down on cryptocurrency businesses by making it difficult for persons to trade in them. Banks and payment providers were ordered by the People's Bank of China ("**PBOC**") to close all accounts and cease providing any services to businesses operating in the cryptocurrency environment. Since September 2017, initial coin offerings ("**ICOs**") have been banned in China, and the activities of cryptocurrency exchange platforms were also essentially prohibited. Although China has been taking active steps to prevent the use of decentralised cryptocurrencies, the PBOC has been considering the adoption of its own digital currency under the control of the Chinese government. To this effect, the PBOC established a Digital Currency Research Institute to investigate the possibility of a national virtual currency.

In contrast to China, Japan decided not to prohibit cryptocurrency exchanges, and instead introduced regulations that help protect users and encourage confidence in the industry. Under the amended Payment Services Act of Japan, operators of cryptocurrency exchanges must be registered with the Financial Services Agency in order to operate, and must comply with various laws, regulations and guidelines. This includes providing regular reports to the Financial Services Agency, keeping customers' money segregated and disclosing certain information to customers. Potential changes to the regulations are

26 https://www.mayerbrown.com/sfc-announcements-on-regulatory-approach-to-virtual-assets-11-09-2018/.

under consideration in order to further tighten controls over cryptocurrency exchanges. Such changes are being considered to be made under the purview of the Financial Instruments and Exchange Act.

On the one hand, stringent regulations work to increase investor confidence and may help bolster the industry, but on the other hand, they could act as a roadblock to the development of cryptocurrencies.

Takeaway

Can there be a possibility of over regulation, which could stifle the industry and be counter-productive? How far should the regulators go to seek to protect investors who enter the cryptocurrency world in full knowledge of the volatility and risky nature of the industry? When cryptocurrency exchanges are faced with security breaches, theft and accusations of fraud, the authorities' reaction is to either introduce tighter regulations or prohibit the operation of such exchanges. Could this come at the expense of innovation and progression?

Many jurisdictions that have sought to regulate cryptocurrency exchanges have largely tried to fit them into pre-existing regulations, e.g. those governing securities or futures contracts. However, the nature of cryptocurrency and the related activities may not be conducive to such regulations. Governments may need to look into the possibility of developing a separate regime or consider relying on self-regulation by industry groups, in order to try and strike a happy balance between investor protection and the benefits of virtual assets. ◆

Contact Us

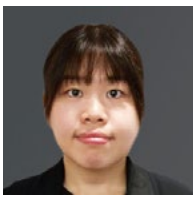
GABRIELA KENNEDY
Partner
+852 2843 2380
gabriela.kennedy@mayerbrown.com

AMITA HAYLOCK
Counsel
+852 2843 2579
amita.haylock@mayerbrown.com

VIVIAN OR
Senior Associate
+852 2843 2510
vivian.or@mayerbrown.com

BENJAMIN CHOI
Partner
+852 2843 2555
benjamin.choi@mayerbrown.com

KAREN H. F. LEE
Senior Associate
+852 2843 4452
karen.hf.lee@mayerbrown.com



ROSANA SHE
Registered Foreign Lawyer
+852 2843 2303
rosana.she@mayerbrown.com

About Mayer Brown

Mayer Brown is a distinctively global law firm, uniquely positioned to advise the world's leading companies and financial institutions on their most complex deals and disputes. With extensive reach across four continents, we are the only integrated law firm in the world with approximately 200 lawyers in each of the world's three largest financial centers—New York, London and Hong Kong—the backbone of the global economy. We have deep experience in high-stakes litigation and complex transactions across industry sectors, including our signature strength, the global financial services industry. Our diverse teams of lawyers are recognized by our clients as strategic partners with deep commercial instincts and a commitment to creatively anticipating their needs and delivering excellence in everything we do. Our "one-firm" culture—seamless and integrated across all practices and regions—ensures that our clients receive the best of our knowledge and experience.

Please visit www.mayerbrown.com for comprehensive contact information for all Mayer Brown offices.