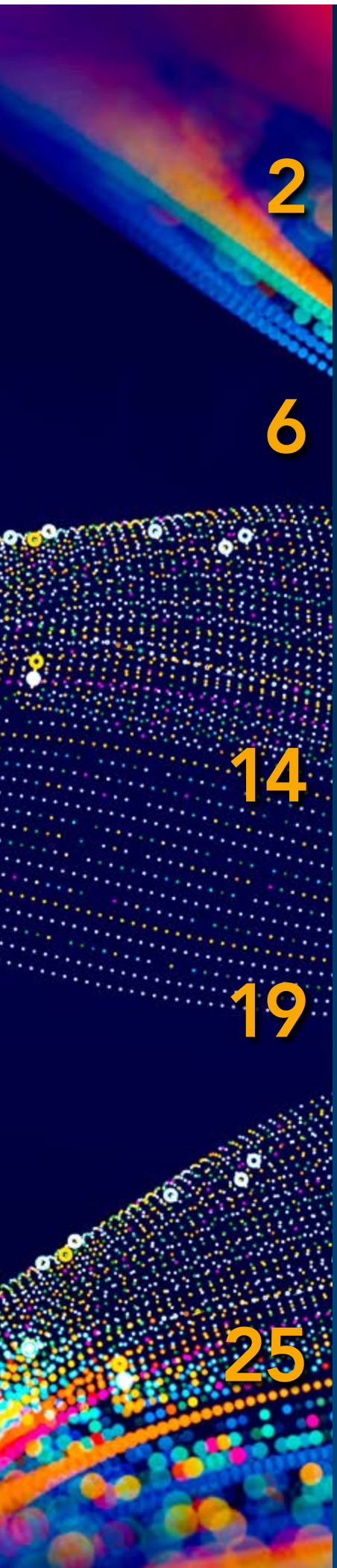
MAYER | BROWN

IP & TMT Quarterly Review

First Quarter 2022

Contents



At Last – China Publishes Revised Cybersecurity Review Measures

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

Joshua Woo, Registered Foreign Lawyer (Singapore)
Mayer Brown, Hong Kong

Introduction and Background

On 4 January 2022, the Cyberspace Administration of China ("**CAC**") published the much anticipated revised Cybersecurity Review Measures ("**Measures**") which set out more information on the cybersecurity review process that will be conducted on (i) network platform operators conducting data handling activities that affect or may affect national security (ii) Critical Information Infrastructure ("**CII**") operators that procure network products and services that influence or may influence national security and (iii) certain network platform operators when listing abroad.

The CAC's move to publish the Measures comes as Didi ChuXing, China's ride hailing giant, plans to delist from the New York Stock Exchange and move its listing to Hong Kong due to pressure from the CAC following concerns over data security. The CAC has been conducting a cybersecurity review of Didi since 2 July 2021, just 2 days after Didi's US$4.4 billion initial public offering ("**IPO**") in New York.

Scope of Application

NETWORK PLATFORM OPERATORS

The Measures will apply to network platform operators handling personal

information of more than one million users in China, who plan to raise funds abroad through IPOs[1] and to such operators that conduct data handling activities that influence or may influence national security[2]. The Measures do not provide a definition for "network platform operators" nor "data handling activities". However, the Online Data Security Management Regulations (Draft for Comment) issued on 14 November 2021, defines "internet platform operators"[3] as data handlers that provide users with internet platform services such as information publishing, social networking, market transactions, payments and audio-visual services. With reference to this definition, the scope of network platform operators is likely to refer to operators who provide similar services via a network. "Data handling activities" is broadly defined under the Data Security Law to include "the collection, storage, use, processing, transmission, provision, disclosure, etc., of data"[4].

Of note is the fact that the Measures do not explicitly address listings by companies in Hong Kong. The Measures cover operators seeking "foreign listing" ("国外上市"). The use of the term "国外", which literally means "outside the country", as opposed to "境外", which generally refers to territory outside of mainland China, suggests that Mainland companies that pursue IPOs in Hong Kong may be exempt from the Measures and the cybersecurity review process. However, the possibility remains that listings in Hong Kong will also be subject to cybersecurity reviews if such listings are considered threats to national security[5].

The Measures are also silent on the types of public listings that will be subject to a cybersecurity review. Accordingly, other types of non-IPO listings such as reverse takeovers, Special Purpose Acquisition Company ("**SPAC**") and direct listings may also be subject to cybersecurity reviews if the network platform operators meet the thresholds stated above. There is no direct reference in the Measures to them having retrospective effect and therefore applying to companies already listed overseas. Rather, the Measures leave the door open for the application of the Measures where "*network products and services as well as data handling activities that the cybersecurity review work mechanism member units believe affect or could affect national security*" are involved[6].

CRITICAL INFORMATION INFRASTRUCTURE OPERATORS

The cybersecurity review also applies to CII operators when they procure network products and services that influence or may influence national security[7]. CII operators are required to assess any potential national security risks arising from the use of network products or services when procuring such products or services[8]. Under the Measures, "network products and services" mainly refers to "*core network equipment, important telecommunications products, high-performance computers and servers, large-capacity storage devices, large-scale databases and application software, cybersecurity equipment, cloud computing services, and other important network products and services that have important influence on the security of CII, cybersecurity and data security*"[9].

Applications for a Cybersecurity Review and Required Materials

Where the Measures apply, CII and network operators will have to file an application for a cybersecurity review with the Office for Cybersecurity Review ("**OCR**"), an office affiliated with the CAC.

When applying for a cybersecurity review, operators must provide[10]:

1 Article 7 of the Measures.
2 Article 2 of the Measures.
3 Article 73(9) of the Draft Online Data Security Management Regulations.
4 Article 3, Data Security Law.
5 Article 16 of the Measures.
6 *ibid.*
7 Article 2 of the Measures.
8 Article 5 of the Measures.
9 Article 21 of the Measures.
10 Article 8 of the Measures.

1. A written declaration;
2. An analytic report on the impact or potential impact to national security;
3. A procurement document, agreement, contract to be signed, IPO materials prepared for submission, and other such listing application documents;
4. Other materials required for cybersecurity reviews.

The Measures provide that the OCR may request further documents from the applicant operator[11]. The Measures further provide that the relevant institutions involved in the cyber security review shall keep confidential the information and documents they received in the course of the review[12].

Review Process Timeline

The following are the 5 main stages of a cybersecurity review under the Measures:

1. The operator must submit an application with the relevant documents.
2. Within 10 working days of the OCR receiving the application and the supporting documents for a cybersecurity review, it must determine whether a review is required and notify in writing the relevant operator of its decision[13]. In the event that no review is required, the company may proceed with its listing overseas.
3. If the OCR deems it necessary to launch a cybersecurity review, it shall complete a preliminary review within 30 working days from the date of issuance of the written notice[14]. In complex cases, the time allowed for preliminary reviews may be extended by 15 working days. This preliminary review will involve suggesting review conclusions and recommendations and transmitting the same to the member units and other departments of the cybersecurity review initiative for opinions.
4. Within 15 working days from receipt of the preliminary review, the relevant member units and departments shall respond with their written comments. If the member units and departments (including the OCR) are in agreement, the OCR shall notify the applicant of the conclusions of the cybersecurity review in writing. If the opinions are conflicting, the case will go through a special review procedure (Stage 5, below).
5. If the member units and relevant departments do not reach a unanimous decision, the case will go through a special review procedure, which shall generally be completed within 90 days although the time for the special review may be extended in more complicated cases.[15]

All in all, the cybersecurity review process may take up between 70 days to 160 days depending on the complexity of the case. Following the review, if the OCR determines that national security will not be affected, the operator can proceed with the listing. Significantly, the Measures allows the OCR, members and departments involved in the cybersecurity review work mechanism to initiate a cybersecurity review even before receiving an application, if they identify network products and services as well as data handling activities that affect or may affect national security[16].

Factors Considered when Assessing National Security Risks

The cybersecurity review process will take into consideration following factors:

1. The risk that the use of products and services could bring about the illegal control of, interference with, or destruction of CII;
2. The harm to CII business continuity of product and service supply disruptions;
3. The security, openness, transparency, and diversity of sources of products and services;
4. The reliability of supply channels, as well as the risk of supply disruptions due to political, diplomatic, and trade factors;
5. Product and service providers' compliance with

11 Article 15 of the Measures.
12 Article 17 of the Measures.
13 Article 9 of the Measures.
14 Article 11 of the Measures.
15 Article 13 of the Measures.
16 Article 16 of the Measures.

Chinese national laws, regulations, and department rules;

6. The risk that core data, important data or large amounts of personal information are stolen, leaked, damaged, or illegally used or illegally exported;
7. The risk existing that due to listing, CII, core data, important data, or large amounts of personal information are affected, controlled, or maliciously used by foreign governments, as well as cybersecurity risks;
8. Other factors that could harm CII security, cybersecurity and data security.[17]

Further Measures for Cybersecurity Review Applicants

The Measures also require cybersecurity review applicants to adopt "*risk prevention and mitigation measures according to cybersecurity review requirements*" during the cybersecurity review process[18]. It is presently not clear what preventive and mitigating measures applicants are expected to take voluntarily. However, the CAC's actions during the cybersecurity review of Didi, which included the removal of Didi's application from smartphone application stores in China and prohibiting Didi from registering new users, indicates that government agencies involved in the cybersecurity review work mechanism possess wide ranging powers to impose preventive and mitigating measures that may directly impact an applicant's business.

Conclusion and Takeaways

The Measures are likely to impact a number of Chinese data-rich companies which may wish to list in overseas markets, such as the United States. So far, both ByteDance Ltd (owner of Tik-Tok) and Ant Group-backed Hello have postponed their respective listings overseas.

The Measures may prove to be a boon for Hong Kong, if no cybersecurity review is required for listings in the special administrative region.

*The authors would like to thank **Thibault Hardy-Abeloos**, Trainee Solicitor at Mayer Brown, for his assistance with this article.*

17 Article 10 of the Measures.

18 Article 16 of the Measures.

The (Algo)Rithm of the Night – China's New Internet Information Service Algorithmic Recommendation Management Provisions

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

Joshua Woo, Registered Foreign Lawyer (Singapore)
Mayer Brown, Hong Kong

Introduction

The Cyberspace Administration of China ("**CAC**"), the State Administration for Market Regulation ("**SAMR**"), the Ministry of Public Security, and the Ministry of Industry and Information Technology have jointly issued a new regulation - the Internet Information Service Algorithmic Recommendation Management Provisions (the "**Provisions**") - to regulate online algorithm recommendation services as part of their latest efforts to rein in Big Tech companies operating in China. The Provisions are scheduled to take effect from 1 March 2022, and will apply to "internet information services"[19] including social media, advertising, e-commerce, and news platforms.

19 Article 1 of the Provisions.

Background

In recent years, China has stepped up its efforts to oversee and regulate the technology sector and the flow of data within and outside China. Concerns over discriminatory recommendation models and opaque data storage practices have been addressed in the Personal Information Protection Law, Cybersecurity Law, Data Security Law, as well as regional regulations such as the Shenzhen Data Protection Regulations.

In particular, China has been proactive in targeting individual companies. In 2021, Meituan, China's leading food delivery platform, was fined 3% of its 2020 domestic revenue, or 3.44 billion yuan (US$533 million), for monopolistic practices. The SAMR followed this with the publication of an administrative guidance, instructing Meituan to rectify its algorithm rules and commission charging mechanism. Similarly, the CAC's cybersecurity investigation against ride-hailing Didi ChuXing's initial public offering rattled the company and caused its swift delisting from the New York Stock Exchange.

It was against this regulatory backdrop that the CAC released a draft consultation on the Provisions on 27 August 2021. The draft Provisions specifically target algorithm recommendation technologies such as product recommendations, personalised advertisements, and filtering, which have traditionally led to false traffic, preferential treatment, public opinion manipulation, and controlling trends.

Changes Made to the Draft

Although the final version of the Provisions does not significantly depart from the draft, a few changes have been made. The use of algorithms to harm public benefit is prohibited[20], and algorithm operators are required to proactively prevent the dissemination of harmful information. Those who operate online news outlets must obtain a permit according to the law, and are prohibited from reporting fake news or news not "published by work units in the State-determined scope"[21]. This "State-determined scope" has not been defined in the Provisions, though this is likely reference to the values set out in Article 3 of the Online Publishing Service Management Rules[22]. A new article has also been added to outlaw monopolistic behaviour or unfair competition when providing online news[23].

Protection for the elderly has also been introduced. Algorithm operators which provide services or cater to the elderly are essentially required to ensure that it is *convenient* for the elderly to use the algorithmic services *securely*. The provisions mandate that these operators should provide smart services that are "suited to the elderly", including fraud monitoring and detection mechanisms[24]. This recognizes the elderly as a vulnerable segment of the population that may be more susceptible to online fraud and underscores the consumer protection element of the Provisions. Separately, an effective complaint mechanism must also be implemented for the public to provide feedback on the algorithms[25]. New penalties for non-compliance with the Provisions include termination of operating licenses[26].

Key Provisions

HIGH LEVEL PRINCIPLES

The Provisions provide high-level regulatory principles for algorithm operators[27]. Formulated in usual "government speak" they include obedience with laws and regulations, respect for social morals and values, professional ethics, and a requirement to operate in a fair, transparent, reasonable, responsible and accountable manner. In addition to this, the Provisions also call for mainstream values and self-discipline. In particular, anything that may endanger national security or social stability is prohibited[28]. It is worth noting that many of these

20 Article 6 of the Provisions.
21 Article 13 of the Provisions.
22 http://www.cac.gov.cn/2016-02/15/c_1118048596.htm
23 Article 15 of the Provisions.
24 Article 19 of the Provisions.
25 Article 22 of the Provisions.
26 Article 33 of the Provisions.
27 Article 4 of the Provisions.
28 Articles 5-6 of the Provisions.

values have not been defined in the Provisions, meaning that like many other regulations the Provisions will be very malleable when it comes to enforcement.

The Provisions appear to focus on the rights of individuals, singling out minors, elderly, labourers and consumers as groups of users to be offered more comprehensive protection. The Provisions address the particular susceptibility of minors to internet addiction[29], the tendency for elderly to fall victim to internet fraud[30], the importance of protecting labourers' rights to salary remuneration and vacation[31], as well as vulnerabilities of online consumers in blindly following algorithms recommendations or trends[32]. This is further coupled with a requirement for algorithm operators to put processes in place to address user and public complaints[33] to ensure that individuals have an avenue for redress.

Additionally, the Provisions set out expectations for algorithm service providers to regularly assess their algorithms to ensure that the algorithmic models do not "*violate laws and regulations or ethics and morals*" such as addiction or excessive consumption. Given that some recommendation algorithms are designed to entice users to continue using the application (e.g. Douyin), there is considerable uncertainty as to the bounds of the Provisions e.g. What is "excessive consumption" or "addiction"? How would algorithms ensure that they do not violate ethics or morals?[34] Nevertheless, this may be a more welcome, nuanced approach to the Chinese government's heavy-handed attempts at managing internet and gaming addiction.

SOCIAL NETWORK SERVICES ("SNS")

One industry targeted by the Provisions is that of SNS. The Provisions prohibit the use of algorithms to "over-recommend" or "manipulate" search results or topic lists, exercise control over popular search terms and other arrangements of information or to carry out acts that may influence public opinion[35]. These prohibitions also seemingly complement the Chinese government's clampdown on celebrity fan culture in China.

However, given that many SNS revolve around pushing "trending" and "viral" content to keep users engaged, and advertisers spending – it is not clear how the CAC will carry out such enforcement.

DIFFERENTIATED TREATMENT

The Provisions also prohibit acts of unreasonably differentiated treatment, furthering the CAC's drive to foster a more competitive marketplace for small and medium enterprises and consumers alike. On the one hand, the Provisions prohibit unreasonable restrictions on other Internet information service providers in a bid to target anti-competitive practices and prevent the abuse of dominant positions[36]. On the other hand, the Provisions offer protection for consumers' fair trading rights by forbidding analytics of consumer purchasing habits to offer them goods and services in a discriminatory manner[37]. This refers to practices Chinese online platforms have been known to employ through price discrimination models based on consumers' price tolerances informed by the consumers' previous purchases and online behaviour. This lack of algorithmic transparency has resulted in higher prices for customers whose purchase history may suggest a higher budget or a recurring need, which goes against the spirit of the Provisions.

CONSUMER RIGHTS

Notably, consumers are now empowered with choice. Consumers have the right to turn off the algorithm recommendation services, or request the service provider to provide services not targeting their personal characteristics[38]. Consumers also have the right to request the service provider to

29 Article 18 of the Provisions.
30 Article 19 of the Provisions.
31 Article 20 of the Provisions.
32 Article 21 of the Provisions.
33 Article 22 of the Provisions.
34 Article 8 of the Provisions.
35 Article 9 of the Provisions.
36 Articles 14-15 of the Provisions.
37 Article 21 of the Provisions.
38 Article 17 of the Provisions.

delete user tags targeting their personal characteristics for algorithm recommendation services.

MANAGEMENT REQUIREMENTS

Despite the vagueness of some of the language in the Provisions, more detailed requirements on oversight and management are also set out[39], providing for the implementation of a graded and categorised system of managing algorithmic service providers by requiring online registration. Individuals or entities may submit a complaint to the relevant departments if they suspect a provider to be violating the Provisions.

PENALTIES

Finally, the Provisions set out the scope of legal repercussions to be borne by violators[40], which include a fine of between 10,000 and 100,000 yuan, warnings, suspension of the business, deregistration, revocation of licences and even criminal liability.

Observations

The Provisions demonstrate a greater emphasis now being placed on consumer rights, by mandating that algorithmic recommendation service providers provide users with a convenient option to switch off algorithmic recommendation services and not target their individual characteristics[41], and refrain from using the algorithms to unreasonably differentiate consumer treatment[42]. However, consumer rights appear to be bolstered only insofar as they relate to "internet information services"[43], and not the use of algorithms by government bodies.

The provisions should come as good news to small to medium-sized businesses and market entrants in the internet industry as they are now more comprehensively protected against monopolistic practices which have proved to be significant deterrents for new market entrants to reach out to customers.

Despite the breadth of its application, the Provisions should come as no surprise given the Chinese government's recent efforts to crackdown on content algorithms, and Big Tech in general. The rules expand the reach of Chinese agencies to algorithm operators specifically, and whilst China has always had strict censorship rules, discouraging over-consumption and internet spending goes hand in hand with a desire to disseminate and inculcate sanctioned values.

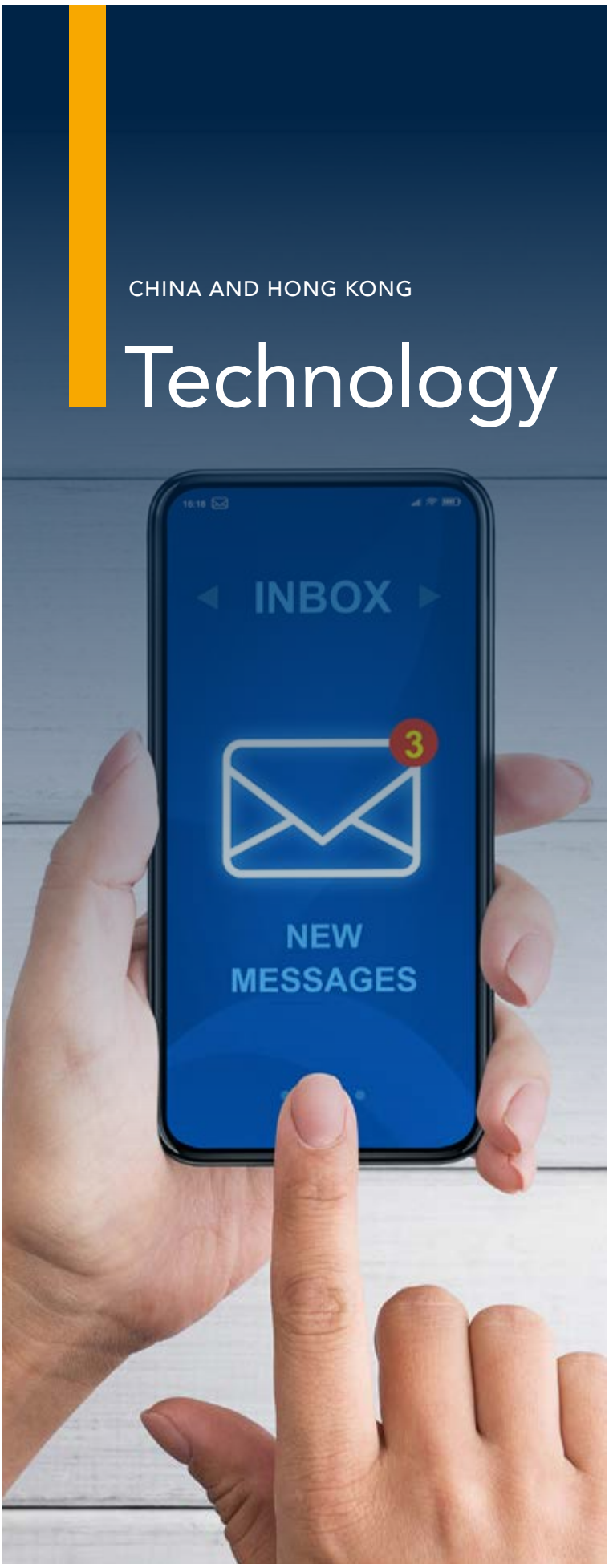
While the penalties brought in by the Provisions which range between 10,000 yuan and 100,000 yuan may seem low especially for large companies[44], the "teeth" of the Provisions lie in the revocation of an algorithm operator's licence and business suspension. Furthermore, many of the existing regulations overlap with the Provisions and regulatory enforcement is likely to culminate in much more severe fines. The Personal Information Protection Law also regulates the way companies handle the personal information of individuals, including their personal data as covered in the Provisions, while the Draft Online Data Security Management Regulations and Data Security Law impose data security requirements on data handlers generally.

Conclusion

The Provisions are expected to have a major impact on all companies relying on algorithms to drive their businesses. Although some of the articles can be vague, companies offering or relying on the use of algorithms to provide services should aim to comply with the Provisions.

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

39 Article 23 of the Provisions.
40 Articles 31-33 of the Provisions.
41 Article 17 of the Provisions.
42 Article 21 of the Provisions.
43 Article 1 of the Provisions.
44 Article 31 of the Provisions.



Pushing the Envelope? The CAC's Draft Regulations on Push Notifications

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

Joshua Woo, Registered Foreign Lawyer (Singapore)
Mayer Brown, Hong Kong

Introduction

On 2 March 2022, the Cyberspace Administration of China ("**CAC**") issued draft regulations on the administration of internet pop-up push notifications (the "**Draft Regulations**"). The Draft Regulations were issued pursuant to a number of laws, including the Cybersecurity Law.

Background

The Draft Regulations were issued in a bid to further tighten government control over the news following a human trafficking controversy that erupted on Chinese social media after a woman was found chained by the neck in Xuzhou last month, and the invasion of Ukraine.

However, the Draft Regulations also address other aspects of push notifications, including the prohibition of algorithmic models that profile minor users and encourage user addiction. This is in keeping with the Chinese government's broader efforts to reduce the influence of Big Tech, and aligns with the recently issued Internet Information Service Algorithmic Recommendation Management Provisions that came into force on 1 March 2022.

The Draft Regulations

SCOPE OF APPLICATION

The Draft Regulations apply to **all** owners and operators of operating systems, terminal devices, application software, websites and other such services ("**Service Providers**") that provide push notification services ("**Push Notification Service Providers**") in China.

TYPES OF INFORMATION NOT ALLOWED

The Draft Regulations sets out various categories of prohibited information in push notifications:

illegal and negative information as defined in the Provisions on Ecological Governance of Network Information Content (the "**Provisions**") that includes content that[45]:

a. opposes the basic principles established by the constitution;
b. endangers national security, divulges state secrets, subverts state power, or undermines national unity;
c. harms national honour and interests;
d. distorts, defames, desecrates or negates the deeds and spirit of heroes and martyrs, or infringes upon the names, likenesses, reputations, or honors of heroes and martyrs by insulting, slandering, or otherwise;
e. advocates terrorism or extremism or incites the commission of terrorist or extremist activities;
f. incites ethnic hatred or ethnic discrimination, undermining ethnic unity;
g. undermines the state's religious policy and advocating cults and feudal superstitions;
h. spreads rumors and disrupts economic and social order;
i. spreads obscenity, pornography, gambling, violence, murder, terror, or instigating crimes;
j. insults or slanders others, infringes upon the reputation, privacy, and other lawful rights and interests of others;
k. uses exaggerated headlines, where the content is seriously inconsistent with the title;
l. hypes up scandals, scandals, bad deeds, and so forth;
m. improperly comments on natural disasters, major accidents, or other disasters;
n. with sexual innuendo, sexual provocation, or other such elements that are likely to cause people to have sexual associations;
o. displays bloody, frightening, cruel, or other such acts that cause people physical or mental discomfort;
p. incites crowd discrimination, regional discrimination, and so forth;
q. promotes vulgar, vulgar, or kitsch content;
r. that might cause minors to imitate unsafe conduct, conduct that violates social morality, induce minors to have bad habits, and so forth;
s. other content that has a negative impact on the network ecology; or
t. other content prohibited by laws or administrative regulations;

ii. information that violates public order and good customs, such as malicious speculation, entertainment gossip, extravagance and ostentation of wealth, and distasteful information[46];
iii. information that maliciously stirs up old news[47];
iv. content that hypes up sensitive events, exaggerate vicious content and disasters, and incites social panic[48].

Push notifications that contain news reports are required to adhere to additional rules such as the fact that the source of news reports must be from the list of 1,358 government-approved news sources published by the CAC in October 2021[49]. This means that news reports from unlicensed sources such as private institutions and individuals cannot be included in push notifications. Accordingly, Push Notification Service Providers need to ensure that push notifications of news reports do not alter the original meaning and content of sanctioned headlines and are traceable

45 Art 6, 7 of the Provisions.
46 Art 5(2) of the Draft Regulations.
47 ibid.
48 Art 5(5) of the Draft Regulations.
49 http://www.cac.gov.cn/2021-10/18/c_1636153133379560.htm

to the original source. Push Notification Service Providers are also required to obtain approval from the relevant source before publishing news contents from news sources in push notifications[50].

Collectively, these prohibitions are very broad and enhance the risks of breaching the law when pushing prohibited news-related notifications or information that may be construed to fall within the above categories.

RESPONSIBILITIES OF PUSH NOTIFICATION SERVICE PROVIDERS

Push Notification Service Providers will be required to put additional processes in place in order to comply with the Draft Regulations.

One such requirement is for Push Notification Service Providers to set up a manual review system[51] for the review of screening, editing, pushing of content and other related work processes. Together with the content prohibitions highlighted in (b), Push Notification Service Providers will have to review the guidelines, policies and processes that they have in place when vetting pushed content.

Push Notification Service Providers are also expected to prioritise user protection and to:

i. clearly inform subscribers of the content and frequency of their push notifications as well as how subscriptions to their push notifications can be cancelled[52];
ii. refrain from differentiating between ordinary users and users who are members when determining the frequency of their push notifications[53];
iii. not interfere with users closing pop-up push notification windows[54];
iv. clearly display the identity of the relevant Push Notification Service Providers in push notifications[55];
v. conspicuously mark "advertisements" to notify users of their nature[56];
vi. allow notifications for advertisements to be closeable with one click[57];
vii. prohibit push notifications that contain links or QR codes to third-party sources[58]; and
viii. establish complaint and reporting avenues[59].

In concert with the Internet Information Service Algorithmic Recommendation Management Provisions that came into force earlier in March, the Draft Regulations also provide further guidance on the use of algorithmic models for push notifications[60]. Push Notification Service Providers are prohibited from using algorithms which induce users to consume excessively, violate laws and regulations and are not ethical. Push Notification Service Providers must not abuse personalised push notifications such as leveraging algorithms to block or over-recommend information. To protect minors, the Draft Regulations also emphasize that algorithms must not be abused to target minors or to subject minors to information that adversely affects their physical or mental health.

PENALTIES

Penalties under the Draft Regulations include warnings, fines, suspension of push notifications and even the suspension of business operations.

50 Art 5(3) of the Draft Regulations.
51 Art 5(6) of the Draft Regulations.
52 Art 5(7) of the Draft Regulations.
53 ibid.
54 ibid.
55 ibid.
56 Art 5(9) of the Draft Regulations.
57 ibid.
58 Art 5(10) of the Draft Regulations.
59 Art 6 of the Draft Regulations.
60 Art 5(8) of the Draft Regulations.

Conclusion and Takeaways

The Draft Regulations apply not just to news organisations but to **all** Push Notification Service Providers which includes any service provider with a mobile application such as shopping centres, banks, gaming companies, food delivery companies etc. All companies with websites accessible in China, or mobile applications downloadable from PRC mobile application stores should review their use of push notifications and associated policies, processes and guidelines.

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

Doxxing Begone: Hong Kong Passes Amendments to the Hong Kong Privacy Law

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

Joshua Woo, Registered Foreign Lawyer (Singapore)
Mayer Brown, Hong Kong

Introduction

The Personal Data (Privacy) (Amendment) Ordinance 2021 ("**Amendment Ordinance**") came into force on 8 October 2021, introducing new provisions to the Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**") to combat doxxing.

Background

Doxxing involves the publishing of private or personal information online without the relevant individual's consent, usually for harassment or other malicious purposes.

Between June 2019 and June 2021, the Hong Kong Privacy Commissioner for Personal Data ("**PCPD**") handled more than 5,800 complaints concerning doxxing, and issued more than 300 *requests* to 18 websites, social media platforms and forums to remove over 6,300 links[61]. In particular, the issue of doxxing was put under a magnifying glass during the 2019–2020 Hong Kong protests, when both protesters and pro-government supporters engaged in doxxing in furtherance of their physical clashes. This resulted in both sides

61 https://www.pcpd.org.hk/english/doxxing/index.html

lodging complaints to the PCPD, though much of the content was placed on servers outside of Hong Kong and therefore outside the territorial reach of the PDPO[62].

Prior to the Amendment Ordinance, there were no direct offences for doxxing in the PDPO, so prosecutors had to rely on other criminal offences to prosecute doxxers e.g. Section 64(2) of the pre-Amendment Ordinance PDPO (the "**Previous Section 64(2)**").

Under the Previous Section 64(2), an offence is only established if a person:

a. Discloses the personal data of an individual *obtained from a data user*;

b. without the data user's consent; and

c. causes psychological harm to the *individual* regardless of intent.

A data user is anyone who controls the collection, holding, processing or use of personal data, which could even be the data subject themselves.

However, since most doxxing cases involve the online circulation of personal data often made 'viral' by forwarding, sharing and reposting, it was difficult for investigators to determine the origin of the personal data, identify the original data user and establish that it had been disclosed "*without the data user's consent*". Prosecutors would also have had to prove harm to the individual and could not have taken into account any impact on the individual's family members, who may have become collateral damage as a result of the doxxing.

Furthermore, the PCPD had limited powers to tackle doxxing activities. Other than the issue of territoriality mentioned above, the PCPD was also not empowered to prosecute doxxers directly and could only refer potential criminal cases to the Department of Justice and Hong Kong Police Force for investigation and prosecution. This made the prevention of doxxing exceedingly difficult; for instance, by the end of June 2021, the PCPD had referred over 1,400 cases to the police for follow-up actions[63], though convictions under the Previous Section 64(2) have been difficult to obtain[64].

In response, the Hong Kong government tabled amendments to the PDPO on 21 July 2021, finally culminating in the passing of the Amendment Ordinance.

Summary

In summary, the Amendment Ordinance tackles doxxing in 3 main aspects:

1. criminalising acts of doxxing under two new direct offences;
2. empowering the PCPD to carry out criminal investigations and prosecution of some offences under the PDPO (including doxxing-related offences); and
3. conferring on the PCPD statutory powers to serve cessation notices to demand actions to cease or restrict disclosure of doxxing content.

Two New Direct Offences of Doxxing

There are two new direct doxxing offences under the Amendment Ordinance – Section 64(3A) and Section 64(3C). Both offences require:

1. disclosure of a data subject's personal data without the data subject's relevant consent; and
2. the establishment of intent or recklessness about whether a specified harm would be or would likely be caused to a data subject or family member of the data subject.

However, the offences can be differentiated on the basis of whether actual "specified harm" has been caused to the data subject or data subject's family members.

"Specified harm" is defined in the Amendment Ordinance to include, in relation to a person: (i) harassment, molestation, pestering, threat or intimidation; (ii) bodily harm or psychological harm; (iii) harm causing that person reasonably to be concerned for his safety or well-being; or (iv) damage to the property of the person.

The definition of "Specified harm" widens the ambit of the potential harm to include "pestering"

62 https://www.pcpd.org.hk/english/news_events/newspaper/newspaper_202001.html

63 https://www.pcpd.org.hk/english/doxxing/index.html

64 https://www.pcpd.org.hk/english/news_events/media_statements/press_20201103.html

and "harassment", which, under the Previous Section 64(2), was limited only to "psychological harm".

SECTION 64(3A)

Section 64(3A) is the "lesser" offence and does not require the disclosure to cause actual "specified harm" – only an intent or recklessness about the likelihood of the specified harm occurring from the disclosure. An offence under Section 64(3A) is punishable with a fine of up to HK$100,000 and imprisonment of up to 2 years.

SECTION 64(3C)

Section 64(3C) is the more serious offence, and, in addition to the intent or recklessness requirement above, requires the disclosure to cause *actual* specified harm to the data subject or any family member of the data subject. An offence under Section 64(3C) is punishable with a fine of up to HK$1,000,000 and up to 5 years' imprisonment.

Power to Carry Out Criminal Investigations and Prosecutions of Doxxing Offences

The Amendment Ordinance also introduces a new range of investigative and enforcement powers in relation to Section 64 offences granted to the PCPD under Part 9A of the PDPO.

Prior to the Amendment Ordinance, the PCPD was not empowered to carry its own investigations or initiate prosecutions. Any doxxing offences under the PDPO had to be referred by the PCPD to the Hong Kong Police Force for investigation and the Department of Justice for *consideration* of prosecution.

The Amendment Ordinance has now expanded the PCPD's investigation and prosecution powers in relation to doxxing to include:

1. the ability to request relevant information, documents or items from anyone, or require anyone to answer relevant questions to assist with any investigation, where the PCPD has reasonable grounds to believe that an offence has been (or is being) committed under section 64 of the PDPO[65];
2. the ability to apply to the court for permission to enter any premises, and to seize documents or items (including mobiles and computers) at the premises, on the basis that the PCPD has reasonable grounds: (i) to suspect that there has been a contravention of Section 64 of the PDPO; and (ii) to suspect that there are documents and things at the premises that can be collected as evidence[66]. Further, under circumstances prescribed in Section 66G(8), the PCPD may even access an electronic device *without* a warrant;
3. the ability to apply to the court for an injunction if the PCPD is satisfied that there is or it is very likely that there is a large scale or repeated contravention of Section 64 of the PDPO in the society[67]. The intent is to prevent the recurrence of doxxing incidents targeting specific persons or groups (e.g. police officers or government officials);
4. the ability to *prosecute* under the PCPD's own name the commission of or conspiracy to commit the following offences:
    a. Section 64(1): disclosure of personal data obtained from a data user without the data user's consent with an intent to obtain gain or cause loss to the data subject;
    b. Section 64(3A) (see 2.1.4(a) above);
    c. Section 66E(1): failure to comply with the PCPD's written notice requiring the provision of assistance and/or materials under Section 66D(2);
    d. Section 66E(5): failure to comply with the PCPD's written notice requiring the provision of assistance and/or materials under Section 66D(2) with an intent to defraud or for purported compliance with a Section 66D(2) requirement by providing material that is false or misleading;
    e. Section 66I(1): obstruction of the lawful exercise of the PCPD's powers under Section 66G in relation to premises and electronic

65 Section 66D of the Amendment Ordinance.
66 Section 66G of the Amendment Ordinance.
67 Section 66P of the Amendment Ordinance.

devices or Section 66H in relation to stop, search and arrest; and

f. Section 66O(1): failure to comply with a cessation notice that requires cessation actions to be taken in relation to a doxxing offence; and

5. the ability to stop, search and arrest, without a warrant, a person reasonably suspected to have committed the doxxing-related offences that are prosecutable by the PCPD mentioned in (4) above[68].

Concerns were raised before the Amendment Ordinance was passed that the PCPD's ability under Section 66D to compel an individual to answer questions from investigation authorities takes away an individual's right to remain silent, as guaranteed by the Basic Law[69]. However, the Amendment Ordinance provides that incriminating evidence obtained by virtue of Section 66D will not be admissible in evidence in criminal proceedings, save for fraud and perjury, if certain conditions under Section 66F are met (i.e. if the individual does not adduce the criminal evidence himself and the PCPD informs the individual of the limitation in this section to the admissibility of incriminating evidence under the PDPO).

Statutory Powers to Serve Cessation Notices

The PCPD is also now empowered to serve cessation notices under the Amendment Ordinance in relation to a Section 64(3A) or (3C) disclosure if:

1. the data subject is a Hong Kong Resident or is present in Hong Kong at the time of the disclosure;
2. there is reasonable ground to believe that a message, whether electronic or otherwise, contains such a disclosure; and
3. a Hong Kong person, or non-Hong Kong service provider, is able to take a cessation action, whether in Hong Kong or not, in relation to the message.

A "Hong Kong person" is widely defined, and refers not just to an individual present in Hong Kong but also a body of persons incorporated, established, registered or that has a place of business in Hong Kong. The provision has extraterritorial effect applying to non-Hong Kong service providers, also broadly defined as a person that has provided or is providing any service (whether or not in Hong Kong) to any Hong Kong person. This would include internet tech giants such as Apple, Amazon, Google and Facebook.

Since a cessation action would include actions to remove the message from an electronic platform, ceasing or restricting access by any person to the message via the relevant platform or discontinuing the hosting service of the part or whole of the relevant platform (e.g. essentially directing an internet platform to take down content), this power has raised freedom of expression concerns. This is particularly so since failure to comply with a cessation notice is a criminal offence, with first time offenders liable to a fine of up to HK$50,000 and up to 2 years' imprisonment, and in the case of a continuing offence (e.g. a circulating subject message), a daily fine of HK$1,000 until the cessation notice is complied with. For subsequent offenders, they may be fined of up to HK$100,000, up to 2 years' imprisonment and a daily fine of HK$2,000 for continuing offences[70].

Nevertheless, there are statutory defences in respect of non-compliance with a cessation notice[71], including:

1. a reasonable excuse for the non-compliance;
2. the nature, difficulty or complexity of compliance;
3. non-availability of technology necessary for compliance; and
4. a risk of substantially prejudicing or causing substantial loss to a third party.

Alternatively, persons served with a cessation notice may lodge an appeal against the notice within 14 days, though they should bear in mind that the cessation notice would still need to be complied with in the meantime[72].

68 Section 66H of the Amendment Ordinance.

69 Letter from the Hong Kong Law Society to the Government regarding the Amendment Bill: https://www.hklawsoc.org.hk/-/media/HKLS/pub_e/news/submissions/20210818.pdf

70 Section 66O(1) of the Amendment Ordinance.

71 Section 66O(2) of the Amendment Ordinance.

72 Section 66N of the Amendment Ordinance.

The PDPO provides immunity from civil liability arising solely from any compliance with a cessation notice[73].

Conclusion

The newly introduced offences and the PCPD's new powers of enforcement are a welcome development in the prevention of doxxing. In December 2021 the PCPD made the first arrest under the Amendment Ordinance.

Businesses, particularly online platform operators, service providers and other publishers of third-party content should bear in mind the obligations introduced by the Amendment Ordinance particularly given their extra-territorial effect.

*The authors would like to thank **Thibault Hardy-Abeloos**, Trainee Solicitor at Mayer Brown, for his assistance with this article.*

73 Section 66P of the Amendment Ordinance.

Proposal to Implement the Arrangement on Reciprocal Recognition and Enforcement of Judgments in Civil and Commercial Matters

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

Background

In 2019, the Hong Kong Government and the Supreme People's Court of the People's Republic of China signed the Arrangement on Reciprocal Recognition and Enforcement of Judgments in Civil and Commercial Matters by the Courts of the Mainland and of the Hong Kong Special Administrative Region (the "**REJ Arrangement**")[74]. The objective of the REJ Arrangement is to reduce the need to re-litigate the same disputes in both Hong Kong and Mainland China by establishing a more comprehensive mechanism for reciprocal recognition and enforcement of judgments in civil and commercial matters between both jurisdictions.

More recently, on 17 December 2021, Hong Kong's Department of Justice released a

74 See our article titled Intellectual Property and Mutual Recognition and Enforcement of Awards between Mainland China and Hong Kong – A New Era?: https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2019/03/asi_ip_tmt_quarterlyreview_2019q1.pdf

public consultation paper on the proposals for the implementation of the REJ Arrangement (the "**Consultation Paper**")[75], for which, the consultation process ended on 31 January 2022. The Consultation Paper sets out a bill, which embodies a legal scheme to implement the REJ Arrangement (the "**Bill**").

In drafting the REJ Arrangement, reference was made to the former draft Hague Convention on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters ("the **Hague Convention**"). Its intention is to provide a single global framework for the circulation, and enforcements, of judgements on both civil and criminal matters across many jurisdictions. The Department of Justice highlighted that, unlike the Hague Convention, the REJ Arrangement also specifically covers judgments involving disputes over intellectual property rights ("**IPRs**").

This article looks at the Bill and proposals contained in the Consultation Paper.

Registration of Mainland Judgments in Hong Kong

In short, under the proposed mechanism in the Consultation Paper:

1. a person may apply to the Court of First Instance ("**CFI**") to have a Mainland judgment in a civil or commercial matter registered with the CFI on an *ex parte* basis;
2. the CFI may set aside the registration, if the applicant has proved to the satisfaction of the court that any of the exhaustive grounds of refusal exists;
3. subject to restrictions in relation to IPRs, the proposed legislative scheme covers both monetary (excluding punitive or exemplary damages) and non-monetary relief; and
4. a registered judgment may be enforced in the same way as if it were a judgment originally given by the CFI.

In the proposed legislative scheme contained in the Consultation Paper, Hong Kong courts would also be empowered to issue certified copies and certificates of Hong Kong judgments[76]. The purpose of these certified copies and certificates is to facilitate a party in seeking recognition and enforcement in Mainland China of a Hong Kong judgment pertaining to a civil or commercial matter.

It is important to note that judgments regarding the validity of an arbitration agreement, and the setting aside of an arbitral award, are excluded from the REJ Arrangement. The Arrangement Concerning Mutual Enforcement of Arbitral Awards between the Mainland and the Hong Kong Special Administrative Region (2000), together with its November 2020 Supplemental Arrangement, continue to be relevant for all arbitration matters.

Setting Aside Registration of a Mainland Judgment in the CFI

The proposed mechanism in the Bill is not necessarily final with regard to registration of a Mainland judgment in the CFI. Mainland judgments registered with the CFI may be set aside, upon application by the person against whom a registered judgment may be enforced[77]. The application to set aside the Mainland judgment must be made within the time limit specified by the CFI. Article 22(1) of the Bill exhaustively sets out grounds pursuant to which the registration must be set aside, for example, where the jurisdictional requirement is not satisfied in the circumstances of proceedings in which the Mainland judgment was given[78] or if the IPRs to which the judgment relates do not fall under the regime of the REJ Arrangement (see below).

Where the original Mainland court proceedings were contrary to a valid arbitration, or jurisdiction agreement entered into by the same parties on the same cause of action, the CFI **may** set aside the

75 The Mainland Judgments in Civil and Commercial Matters (Reciprocal Enforcement) Bill and the Mainland Judgments in Civil and Commercial Matters (Reciprocal Enforcement) Rules Consultation Paper: https://www.doj.gov.hk/en/featured/pdf/consultation_paper_on_the_mainland_judgments_e.pdf

76 Articles 33 and 34 of the Bill.

77 Article 21 of the Bill.

78 The jurisdictional requirements are detailed in Articles 23 of the Bill.

judgment, on a discretionary basis[79].

It is important to bear in mind that an action to enforce a registered Mainland judgment may be taken only after:

a. the expiry of the period within which an application to set aside the registration of the judgment may be made; or
b. when an application to set aside has been made, the application has been finally disposed of[80].

Judgments Concerning IPRs and Exceptions

As previously noted, the REJ Arrangement covers judgments concerning IPRs, although this is subject to some broad exceptions. The Bill contains a number of provisions applicable to Mainland judgments, concerning "specified intellectual property rights", defined in Article 2 of the Bill as:

> *"a. a copyright or related right;*
>
> *c. a trade mark;*
>
> *d. a geographical indication;*
>
> *e. an industrial design;*
>
> *f. a patent;*
>
> *g. a layout-design (topography) of integrated circuit;*
>
> *h. a right to protect undisclosed information; or*
>
> *i. a right enjoyed by a person in respect of a new plant variety under subparagraph (7) of the second paragraph of Article 123 of the Civil Law Code of the PRC)."*

The definition of "specified intellectual property rights" is the same as Article 1(2) of the 1995 Agreement on Trade-Related Aspects of Intellectual Property Rights, save that it is the first time that plant variety rights are also recognized as an IPR.

The specific scope of judgments involving IPRs covered or excluded (as the case may be) by the REJ Arrangement are as follows[81]:

a. judgments ruling on contractual disputes involving IPRs are covered;
b. judgments ruling on tortious claims for infringement of IPRs are covered, except for infringement of invention patents and utility models in the Mainland and infringement of standard patents (including "original grant" patents) and short-term patents in Hong Kong;
c. judgments ruling on the licence fee rate of standard essential patents in both the Mainland and Hong Kong are excluded; and
d. a ruling on the validity, establishment or subsistence of IPRs is not recognised or enforced under the REJ Arrangement.

For most types of judgments, the REJ Arrangement covers both monetary (including exemplary or punitive damages) and non-monetary relief. The exception is judgments ruling on tortious claims for infringement of IPRs, including acts of unfair competition prohibited under Article 6 of the Anti-Unfair Competition Law of the People's Republic of China but excluding tortious claims for infringement of trade secrets[82], whereby the REJ Arrangement only covers monetary relief (including exemplary or punitive damages)[83]. This means that judgments awarding injunctions relating to tortious claims for infringement of IPRs will not be recognized.

Despite the broad definition of "specified intellectual property rights" and the restriction in respect of tortious disputes, cross-border parties to IPR litigation will be able to benefit from the REJ Arrangement.

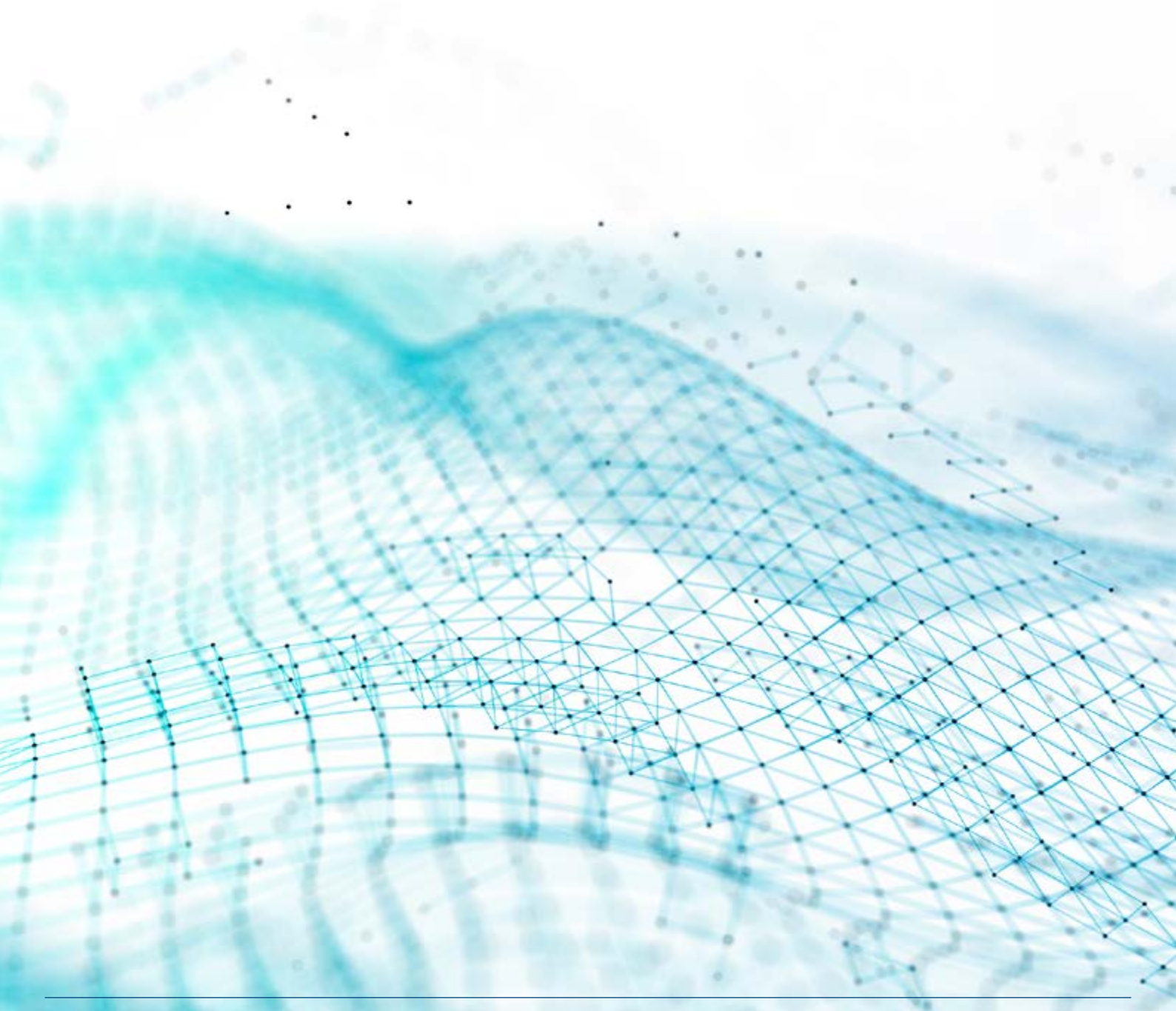
Conclusion

The Bill significantly enhances cooperation between Hong Kong and Mainland China's legal systems. The Bill reinforces Hong Kong's position as a competent jurisdiction to deal with legal disputes with a Mainland China connection. However, in relation to IPRs, the scope of the Bill is limited as it specifically excludes Mainland judgments ruling on the validity, establishment or subsistence of IPRs

79 Article 22(2) of the Bill.
80 Articles 27 of the Bill.
81 Articles 3(1)(3) and 15 of the REJ Arrangement.
82 Article 17(2) of the REJ Arrangement.
83 Article 17(1) of the REJ Arrangement.

and the recognition of only monetary relief for judgments on tortious claims for IPR infringement cases. Despite its limitations, the Bill remains a step in the right direction for cross-border IP disputes in this part of the world.

The author would like to thank ***Thibault Hardy-Abeloos***, Trainee Solicitor at Mayer Brown, for his assistance with this article.



The Future of Consent Letters for Trade Mark Applications in China

By **Michelle G.W. Yee, Counsel**
Mayer Brown, Hong Kong

Introduction

The Trademark Review and Adjudication Department ("**TRAD**") of the China National Intellectual Property Administration ("**CNIPA**") had, in recent years, begun to take an increasingly permissible approach toward consent letters submitted by applicants to overcome citations of prior similar marks. This promising trend came to an abrupt end around September 2021, when the TRAD unilaterally decided that it would no longer accept consent letters in almost all trade mark review proceedings. This sudden reversal was made informally without prior notice or explanation, and blindsided brand owners and trade mark practitioners alike, many of whom had already spent months negotiating co-existence agreements and arranging for legalised consent letters prior to the policy change.

Consent Letters in Different Jurisdictions

Although trade mark laws can vary greatly from one jurisdiction to another, a fundamental objective underlying most trade mark regimes is to ensure that consumers can clearly differentiate between goods and services offered by different traders under their respective trade marks. The public interest of preventing consumer confusion must be weighed against the idea that

trade marks are property rights whose owners should be allowed to commercially delineate the boundaries of their respective rights in the market.

In jurisdictions such as Hong Kong, the balance is tipped in favour of brand owners – the submission of a signed consent letter from the owner of a cited mark will be accepted by the Trade Marks Registry to overcome a citation objection, even if the respective marks are identical and cover identical goods or services. The EU goes even further, forgoing citation objections altogether and placing the onus on owners of earlier similar marks to oppose applications that they deem concerning.

Other jurisdictions such as Japan take the opposite approach and refuse to accept consent letters at all. Brand owners are forced to enter into so-called "assign-back agreements", whereby the trade mark applicant assigns their mark to the cited mark owner to present a legal fiction that the marks are owned by the same entity in order to overcome a citation objection, after which the mark is assigned back to the applicant.

The Approach in China

In China, the prevention of consumer confusion still outweighs the private interests of brand owners, but the Chinese courts (and, until recently, the TRAD) have shown a willingness to defer to brand owners' intentions and accept consent letters in cases where the marks in question are not identical or very closely similar. The courts' more permissible attitude towards consent letters and co-existence agreements could be seen in the Beijing Higher People's Court's "Guidelines for Administrative Proceedings relating to the Granting and Verification of Trade Mark Rights" (北京市高级人民法院商标授权确权行政案件审理指南) issued in April 2019, which expressly provided that consent letters would be considered to be prima facie evidence that there is no risk of confusion (Article 15.10), although consent alone would not be sufficient in cases where the respective marks are identical or almost identical and cover identical or similar goods or services (Article 15.12).

Consent Letters before TRAD

Under the current system, trade mark applications are first examined by the Trade Mark Office of the CNIPA, which will provisionally refuse an application if it is found to be identical or confusingly similar to an earlier mark in respect of identical or similar goods or services (amongst other grounds for refusal). The applicant can contest the refusal by filing a review with the TRAD, at which stage a notarised and legalised consent letter signed by the owner of the earlier mark could be submitted for consideration. The TRAD's abrupt policy change means that consent letters submitted during review proceedings are now unlikely to be sufficient to overcome the refusal.

The TRAD has made no official announcements to explain their rationale for the change, nor have they stated whether there are circumstances (if any) in which consent letters may still be accepted (for example, it is unclear whether consent letters issued by an affiliate of the applicant might still be acceptable).

What Should Brand Owners Do?

Although the TRAD has changed its attitude to consent letters, the courts have yet to follow suit. Brand owners who have negotiated co-existence with cited mark owners should therefore be prepared to appeal their cases to the courts. It would also be advisable for brand owners to arrange for the execution and legalisation of two sets of consent letters, the first for submission to the TRAD during the review stage, and the second to be retained for the eventual court appeal.

It should also be noted that the TRAD is prone to abrupt policy changes, and may reverse their stance yet again in the near future. Brand owners should continue to consider consent letters as an option for overcoming cited marks (particularly where written arguments are unlikely to succeed), bearing in mind they will likely need to budget additional time and costs for filing court appeals.

Contact Us

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

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

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

Joshua Woo
Registered Foreign Lawyer (Singapore)
+852 2843 4431
joshua.woo@mayerbrown.com

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 mayerbrown.com for comprehensive contact information for all Mayer Brown offices.