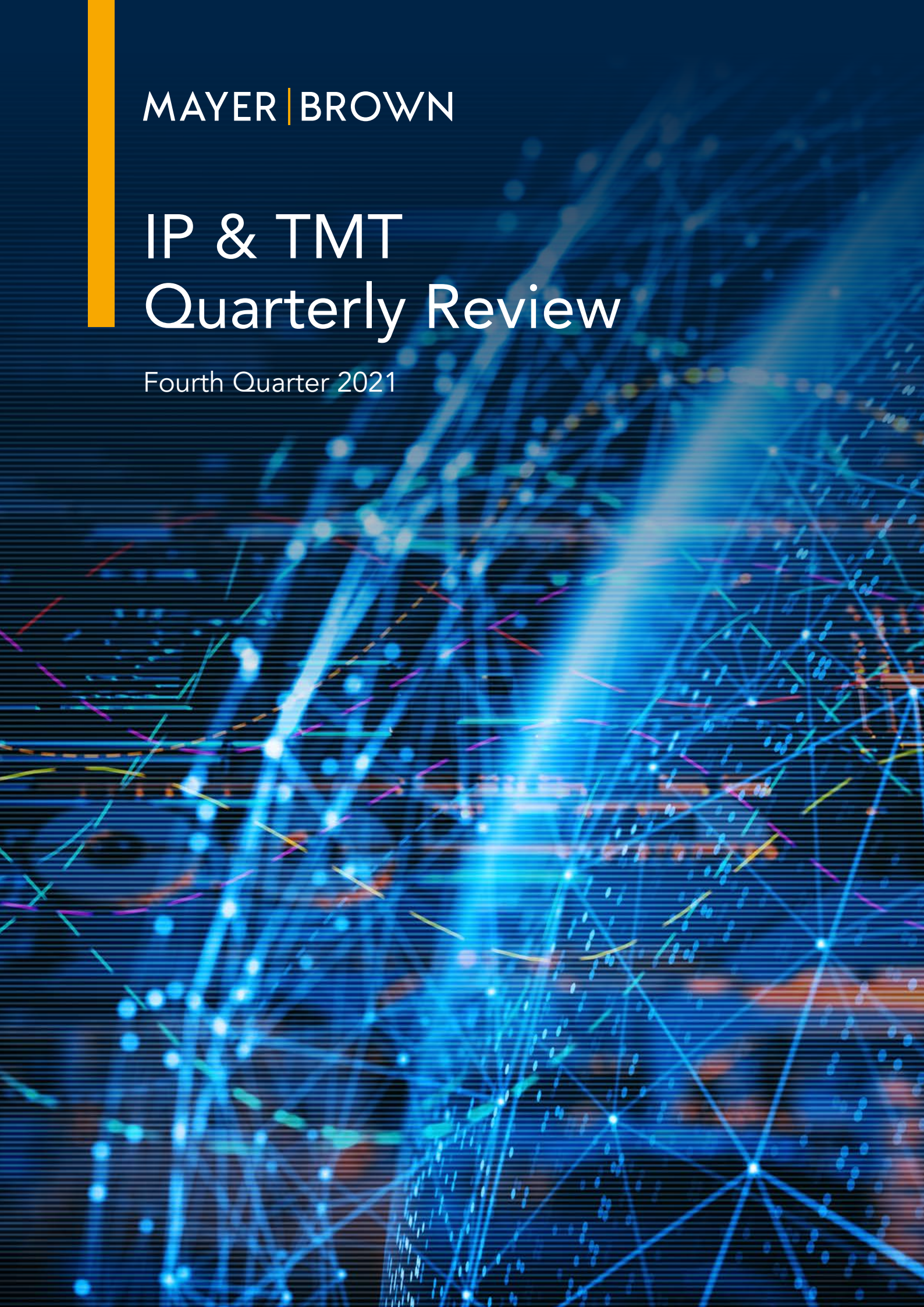
MAYER | BROWN

IP & TMT Quarterly Review

Fourth Quarter 2021



Contents

2 Data Privacy
Hong Kong and China
DATA PRIVACY BEYOND BORDERS: PCPD ISSUES JOINT STATEMENT ON GLOBAL PRIVACY EXPECTATIONS OF VIDEO TELECONFERENCING COMPANIES
CLASSIFYING DATA: CHINA ISSUES DRAFT MEASURES FOR THE ADMINISTRATION OF DATA SECURITY IN INDUSTRY AND INFORMATION AREAS

8 Intellectual Property
Hong Kong and China
MEASURES FOR THE ADMINISTRATION OF LISTS OF SERIOUS ILLEGAL AND DISHONEST ACTS SUBJECT TO MARKET REGULATION
AT LAST – RENEWED ATTEMPTS TO UPDATE HONG KONG'S COPYRIGHT ORDINANCE

14 Arbitration
Hong Kong
HONG KONG COURTS CONTINUE TO TAKE A PRO-ARBITRATION APPROACH

17 Artificial Intelligence
China
CHINA ANNOUNCES THREE-YEAR PLAN TO STRENGTHEN THE MANAGEMENT OF ALGORITHMS
HUMANS VERSUS ROBOTS: CHINA RELEASES ETHICAL GUIDELINES ON THE USE OF ARTIFICIAL INTELLIGENCE

23 Cybersecurity
China
CHINA ISSUES DRAFT NETWORK SECURITY MANAGEMENT REGULATIONS

27 Contact Us

HONG KONG AND CHINA

Data Privacy

Data Privacy Beyond Borders: PCPD Issues Joint Statement on Global Privacy Expectations of Video Teleconferencing Companies

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

Cheng Hau Yeo, Associate
Mayer Brown, Singapore

The Office of the Privacy Commissioner for Personal Data ("**PCPD**") joined forces with data protection authorities from Australia, Canada, Gibraltar, Switzerland, and the United Kingdom (collectively the "**Joint Signatories**") to publish a statement on 27 October 2021, titled "Observations following the joint statement on global privacy expectations of video teleconferencing ("**VTC**") companies".

The joint statement is described by Ms. Ada Chung Lai-ling, the Hong Kong Privacy Commissioner of Personal Data , as a "concluding report on a series of engagement activities since July 2020 between the PCPD, together with five data protection authorities, and four of the biggest VTC companies, namely Cisco, Google, Microsoft and Zoom". It aims to address privacy concerns following the rise in the use of video teleconferencing applications during the pandemic.

Five Areas of Good Practice

The Joint Signatories highlighted five key areas where VTC companies have engaged in "good practice" when implementing their privacy controls: "Security", "Privacy-by-design and default", "Know your audience", "Transparency", and "End-user control".

- **Security** – VTC companies have reportedly carried out several methods of security testing including carrying out penetration tests, using open source code to enable third party scrutiny, engaging in threat modelling, obtaining internationally recognised certifications, implementing "bug bounty" programs, and conducting independent audits. In this regard, the Joint Signatories recommended adopting a multi-pronged approach when implementing security measures. Moreover, the Joint Signatories also found that good practices have been introduced vis-à-vis employees and third-party sub-processors to ensure the safe handling of personal information – these include conducting regular audits of third parties, carrying out pre-employment checks, and limiting employee access to only data that is strictly required for their particular job functions.
- **Privacy-by-design and default** – Privacy programs, such as regular contact between privacy teams and completion of privacy impact assessments, were also highlighted in the joint statement. In particular, the Joint Signatories noted the good practice of setting the default controls to the most protective setting possible, including having virtual waiting rooms, passwords requirements, and video and microphone switched off.
- **Know your audience** – VTC companies must "know their audience" given that there has been an increasing use of VTC applications within sensitive sectors, such as education and healthcare. Some good practice were noted including sole teacher control of screen sharing as well as secure screen sharing of health and medical documents. The Joint Signatories also recommended popularising the use of tailored privacy settings for specific industries by adopting custom guidance for school administrators, parents, and enterprise clients.
- **Transparency** – It is vital to keep users informed on how and why their data is being collected and stored. A multi-pronged approach has been reported to be taken by various VTC companies, which combines measures such as providing contextual notices, dashboards delineating different types of personal data collected, and pop-ups during calls. Moreover, the report emphasises third-party involvement in data handling, and adopting good practices such as having a 6-month notification period prior to the use of new third party processors – a practice already introduced by various VTC companies.
- **End-user control** – Finally, the Joint Signatories note that users must be given unambiguous controls when interacting with VTC services. Examples of good practices already implemented include the ability to opt-out of being included in attendance reports, the requirement of user consent prior to host unmuting audio, and the use of virtual backgrounds. Nonetheless, the Joint Signatories acknowledged that at times users may inadvertently put the data of other participants at risk by sharing the meeting content with third parties. In this regard, some innovative solutions have been identified, such as adopting scanning tools to target and detect any such content on social media.

Recommendations

In addition to highlighting the areas of good practice currently adopted by VTC companies, the Joint Signatories also issued recommendations on improving the current levels of security protection.

The first recommendation is to adopt an encryption standard that is more robust than the industry minimum, as well as an end-to-end encryption tool under appropriate circumstances. Whilst this may restrict the functionality of VTC services, such as users being unable to join by phone, such limitations may be beneficial for highly sensitive meetings that may take place on those platforms. In this regard, the Joint Signatories also recommended allowing users to select their desired type of encryption, with end-to-end encryption being the default for telehealth-related meetings.

The second recommendation is for more explicit notifications to be issued to users when their data is used for secondary purposes not relating to the core operating functions of the VTC software. This should be done in a proactive, unambiguous and

upfront manner. Targeted advertising and tracking cookies should only be allowed with the user's consent.

Lastly, the Joint Signatories recommended that VTC companies should be transparent about the geographical locations where user data is being routed and stored, and wherever possible, they should allow users to choose the jurisdictions where their data is being handled. Additional safeguards, such as contractual agreements, should also be in place when data is shared with recipients in foreign jurisdictions.

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

Classifying Data: China Issues Draft Measures for the Administration of Data Security in Industry and Information Areas

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

Cheng Hau Yeo, Associate
Mayer Brown, Singapore

On 30 September 2021, China's Ministry of Industry and Information Technology ("**MIIT**") released the draft "Measures for the Administration of Data Security in Industry and Information Areas" ("**Draft Measures**") which set out a framework for the regulation of industrial data. In particular, the Draft Measures provide regulatory guidance on how industrial data in China is to be categorised in the context of the Data Security Law ("**DSL**") namely as: 'ordinary', 'important' or 'core'. The categorisation will affect how and whether such industrial data may be transferred outside of China.

Background

The DSL imposes various requirements relating to the collection, processing and transfer of a broad range of data with a specific focus on "important data" and "core data". Since the passing of the DSL concerns have been raised over some of the ambiguities and uncertainties found in the provisions of this law including , those relating to the definitions of the different categories of data. Under the DSL,

regulators at the regional and sectoral levels are tasked with issuing specific catalogues to identify the scope of "important data" in their respective regions or sectors based on the national level data categorisation and classification system.

The Draft Measures, which were open for public consultation until the end of October, seek to clarify some of these uncertainties and provide further details in relation to the obligations under the DSL specifically in the industrial and telecommunications sectors.

In particular, the explanatory note to the Draft Measures sets out three main aims in respect of the industrial and telecommunications industries:

1. To fully implement the requirements of DSL;
2. To develop a data security monitoring system; and
3. To provide further details on data protection requirements.

Key Provisions in the Draft Measures

'Ordinary data' is defined in the Draft Measures as data

a. which has a minimal impact on public interest, individual's or entity's legal rights, and society;
b. which affects a small number of users and companies and has limited impact on business , for a short duration of time, or minimal impact on company management, sector development, and technology advancement;
c. where the costs required to recover such data or to eliminate negative consequences are minimal; or
d. which does not fall within the definitions of 'important' or 'core' data.

'Important data' is defined as data falling under any of the following categories:

a. Threatens 'politics, land, military, economy, culture, society, science and technology, cyberspace, ecosystem, resources, nuclear security' or China's data security in 'space, polar regions, deep sea and artificial intelligence';
b. Affects industrial and telecommunications developments and other economic interests;
c. Causes major data security or production safety breaches, and seriously affects public interest, individual or entity's legal rights, and society;
d. Causes an obvious cascade effect on multiple industries, sectors and companies, for a prolonged period of time, leading to serious consequences to industrial and technological developments;
e. Costs required to recover data or to eliminate negative consequences are significant; or
f. Other data deemed 'important' by the supervising departments.

Finally, 'core data' is defined as data falling under any of the following categories:

a. Seriously threatens 'politics, land, military, economy, culture, society, science and technology, cyberspace, ecosystem, resources, nuclear security' or China's data security in 'space, polar regions, deep sea and artificial intelligence';
b. Seriously affects industrial and telecommunications developments and other economic interests;
c. Causes significant losses to industrial production, telecommunications, and internet services, leading to large-scale network and service paralysis; or
d. Other data deemed 'core' by supervising departments.

All entities holding or processing any industrial data must submit their data categorisation assessments to the MIIT. Entities holding industrial data have to undergo a special review and approval process if they wish to share or transfer any 'important data' outside of China. The Draft Measures impose a blanket prohibition on any sharing or transfer of 'core' data overseas.

The Draft Measures also impose an obligation on organisations to report any emergency data leaks to the relevant authorities. Where such incident affects the legal rights of any users, these users must also be informed of the incident and mitigating actions must be carried out in a timely manner. A complaint system will also be established to detect and counter any activities that violate the relevant data security requirements.

In addition, the Draft Measures set out a list of penalties that may be imposed on an organisation in relation to a breach of its data security obligations. For example, a blacklist will be established to

identify entities that are acting in breach of their data security obligations. Other penalties include a public shaming, forfeiture of illegal proceeds, financial penalties, suspension of business, closure of websites, revocation of registration licenses, and even criminal liabilities.

Takeaways

The Draft Measures (once passed), together with the DSL, will have a significant impact on any business operating in China, especially those operating on a regional or global scale. For example, the Draft Measures and the DSL, may provide ammunition for US-owned companies in China to resist data access requests from US law enforcement authorities pursuant to the Clarifying Lawful Overseas Use of Data Act (which allows US law enforcement authorities to compel access to data owned and controlled by entities under US jurisdiction, even if such data is located outside of their territories); however the bigger question remains as to how such conflicts of law should be handled. Apart from the US, other entities around the world, including intermediaries such as accountancy firms, banks, consultancy firms and law firms, will similarly find it more difficult to access data (particularly important or core data) held by China-based organisations and clients.

Despite the efforts made to provide clarification to the DSL, there are still several uncertainties regarding the DSL that remain unresolved. For instance, the Draft Measures did not specify what would constitute national and economic interests, and left the interpretation of such terms to the local government bodies and ministries. The categorisation process for 'core', 'important' or 'ordinary' data also appears to be a subjective one, with the data categorisation to be determined by the data holders themselves (albeit subject to approval by authorities). It is hoped that the final version of the Draft Measures, following public consultation, will provide a higher degree of granularity in relation to this process. In the meantime, companies that are subject to the DSL are advised to keep an eye out for the final version of the Draft Measures additional or new guidance on the classification and requirements relating to the data they collect and process in China.

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

HONG KONG AND CHINA

Intellectual Property

Measures for the Administration of Lists of Serious Illegal and Dishonest Acts Subject to Market Regulation[1]

By **Michelle Yee, Counsel**
Mayer Brown, Hong Kong

Introduction

In the past few years, the Chinese government has issued a number of regulatory measures to curb rampant trade mark hijacking and intellectual property infringement. In 2019, the China National IP Administration ("CNIPA") issued "Several Measures on Regulating Applications to Register Trade Marks" with the specific aim to reduce the number of bad faith trade mark filings and clarified the CNIPA's internal blacklisting procedure for bad faith filers. On 30 July 2021, the State Administration of Market Regulation ("SAMR") issued two sets of measures to crack down on intellectual property abuse. The first set, "Measures for Collaborative Governance of Violations and Offences in the Patent and Trade Mark Agency Industry"[2], addressed the unethical behaviour of patent and trade mark agents in facilitating bad faith filings and other illegal acts. By contrast, the second set, "Measures for the Administration of Lists of

1 Original text can be found here:市场监督管理严重违法失信名单管理办法_其他_中国政府网 (www.gov.cn)

2 The first set of Measures was discussed in the previous issue of our Quarterly Review, and is available here

Serious Illegal and Dishonest Acts Subject to Market Regulation" (the "Measures"), targets not only agency misconduct, but also a wider range of behaviour in the name of market regulation. This includes actions that distort fair competition, including infringement of intellectual property rights and bad faith trade mark filings, to be dealt with under the China social credit system.

The SAMR also issued a "policy interpretation"[3] to accompany the Measures on 3 August 2021. According to the policy interpretation, the Measures were issued as an update to the interim blacklisting measures that had been in place since April 2016. As institutional structures and the social credit system evolved, these interim measures had become outdated and were in need of an update. By issuing the updated Measures, the SAMR hopes to standardise the various management systems for industry and commerce, quality inspection, food and pharmaceutical safety, and intellectual property protection under a unified approach to tackle a broad spectrum of market misconduct.

Circumstances for Blacklisting

The types of behaviour identified in the Measures that may warrant blacklisting, and factors to be considered when imposing punishment are discussed below.

Articles 2 and 5-11 set out the specific behaviours that may result in blacklisting on the social credit system. Under Article 2, an entity may be blacklisted if it violates any laws or administrative measures in bad faith resulting in serious consequences, and is subject to 'heavy administrative penalties'[4] imposed by the SAMR. Articles 5 and 6 are dedicated to the safety of food and medicine, notably singling out 'vaccines' as one of the regulated products. Articles 7, 8 and 10 address quality control, consumer protection, and business malpractice respectively, while Article 9 covers illegal acts including:

1. trade secret infringement, commercial slander, organisation of false transactions, and other acts undermining fair competition;
2. intentional infringement of intellectual property rights and submission of bad faith trade mark applications;
3. price collusion, failure to implement government pricing guides on goods relating to national economy or emergency price intervention measures;
4. participation in pyramid schemes; and
5. publication of false advertisements relating to goods affecting consumers' health.

Article 11 provides that, where an entity is subject to an administrative decision but refuses to comply with that decision, that entity may be blacklisted even if their original actions did not warrant blacklisting. In effect, non-compliance may "escalate" the original sanctions into being blacklisted.

Article 12 provides useful guidance on factors to be considered when imposing punishment. These include, among others, the existence of subjective bad faith, the frequency and duration of violations, the value of the relevant products, and harm caused to livelihoods, health, and property. It is interesting to note that the SAMR has chosen only to address subjective rather than objective bad faith, which means that proof of subjective intention to cause harm will be required in order for an entity to be blacklisted.

Consequences of Blacklisting

Article 15 sets out the consequences of being blacklisted. Blacklisted entities may have difficulty obtaining administrative licences or securing contracts for infrastructure or other government projects and may also be targeted as key subjects for supervision with increased frequency of inspections. Such entities will be excluded from any commendations or awards, and may also be subject to additional supervision or management measures under various laws and administrative regulations.

Safeguards

Given the serious consequences of blacklisting, the Measures include various provisions to safeguard

3 Original text can be found here: 《市场监督管理严重违法失信名单管理办法》政策解读 (samr.gov.cn)

4 These include: (1) discretionary fines; (2) licence revocation or lowering the qualification level or revoking a licence; (3) restriction, suspension, or closure of business activities or restriction of employment; and (4) other heavier administrative penalties as prescribed by law.

the rights of entities subject to possible sanctions. Under Article 13, the SAMR is required to decide whether the respondent will be blacklisted at the time it issues an administrative decision, and the SAMR must explain the legal basis and reasoning for its decision, and the decision must also set out the respondent's legal rights. Article 22 also requires that a decision made at the county or district level be approved by the supervisory agency one level above – this allows for some oversight of the decision process and could safe-guard against local protectionism or corruption.

A respondent subject to a blacklisting order may apply for administrative reconsideration or initiate administrative proceedings pursuant to Article 23.

Duration of Blacklisting Orders

An order for blacklisting will normally be for three years, but a blacklisted entity may apply for early removal after one year pursuant to Article 16 if it has:

1. complied, on its own accord, with all obligations imposed by the administrative order;
2. proactively remedied any harmful consequences and adverse effects caused by its actions; and
3. not been subject to further severe administrative penalties.

However, if the party applying for early removal deliberately conceals facts and provides false information, the authorities may order the three-year blacklist period to start afresh.

Conclusion

The updated Measures target "market misconduct" by entities conducting business in China – the umbrella term "market misconduct" encompasses a wide range of bad behaviour that could cause harmful consequences to the commercial market. It is likely that the updated Measures were released mainly to address health and safety concerns associated with the recent proliferation of vaccines and other pharmaceutical products. Nevertheless, infringement of intellectual property rights and trade mark hijacking are expressly included as types of market misconduct that are liable to result in blacklisting. Given the serious consequences of being blacklisted on the national social credit system, the Measures will hopefully act as another deterrent to bad faith filers and infringers.

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

At Last – Renewed Attempts to Update Hong Kong's Copyright Ordinance

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

Introduction

In her Chief Executive's 2021 Policy Address, Carrie Lam announced plans "to revive the Copyright Ordinance amendment exercise", in line with the People's Republic of China's 14th Five-Year Plan, which supports the development of Hong Kong as a regional intellectual property trading centre.

Acknowledging the need to update Hong Kong's copyright laws in light of technological developments, on 24 November 2021 the Government launched a three-month public consultation to gauge views on updating Hong Kong's copyright regime. The Government's proposals are set out in a public consultation paper (the "**Consultation Paper**").

Some of the proposals in the Consultation Paper are based on the Copyright (Amendment) Bill 2014, which was shelved in 2016 due to the polarised interests of various stakeholders.

In this article, we look at the key proposals to amend the Copyright Ordinance (Cap. 528) ("**CO**") set out in the Consultation Paper in respect of:

- a new technology-neutral exclusive communication right for copyright owners which would cover new modes of electronic transmission and equivalent criminal sanctions for breach;

- two extra statutory factors to consider when assessing damages in civil cases involving copyright infringement;
- new "safe harbour" provisions for Online Service Providers ("**OSP**") to limit their liability for any rights infringement occurring on their platforms; and
- new copyright exceptions for the use of copyright works.

We also examine the Government's position to retain the current, exhaustive approach to copyright exceptions and the limitations of the Government's position not to introduce copyright-specific statutory provisions for site blocking injunctions.

Technology-Neutral Communication Right and Criminal Liability

The Government has proposed a new exclusive right for copyright owners to communicate their works to the public on any electronic platform. This would enhance the current CO, which only provides for specific methods of communication, such as "broadcasting" or "including the work in a cable programme service". The new right to communicate would be expressed in broad terms, so as to cover current and future methods of electronic transmission. The aim of this communication right would be to tackle online piracy (including streaming) and enhance the copyright protection of digital content.

To bolster this, new criminal sanctions will also be introduced against the unauthorised communication of works to the public in circumstances where the copyright in a work is infringed either (i) for the purpose of or in the course of trade or for profit; or (ii) to such an extent as to affect prejudicially the copyright owner.

Additional Damages in Civil Cases Involving Copyright Infringement

In order to enhance protection for copyright owners in the digital environment, the Consultation Paper recommends the introduction of two new statutory factors to consider when assessing damages in civil cases for copyright infringement. The two factors are (i) the unreasonable conduct of an infringer after having been informed of the infringement; and (ii) the likelihood of widespread circulation of infringing copies as a result of the infringement.

Safe Harbour Provisions

The Government's is also proposing safe harbour provisions for OSPs in relation to copyright infringement on OSP platforms. To benefit, an OSP when notified of a copyright infringement must take reasonable steps to limit or stop the infringement, including reasonable steps to remove the alleged infringing work. These safe harbour provisions strike a balance between protecting creative works for copyright owners and safeguarding the operations of OSPs, and are important to keep the CO up to date with technological developments, in particular the Internet. The CO safe harbour framework will be underpinned by a voluntary Code of Practice which will set out practical guidelines and procedures for OSPs to follow after they receive notification of an alleged copyright infringement.

New Fair Dealing Exceptions

Hong Kong's copyright exceptions are restricted to a specified range of purposes and circumstances, all of which are exhaustively listed in the CO. The CO currently contains over 60 sections which specify acts that are permitted without attracting civil or criminal liability in relation to copyright works. Hong Kong's copyright exceptions are known as "fair dealing" exceptions.

The Consultation Paper proposes introducing new copyright fair dealing exceptions for the use of copyright works for three categories - namely (i) parody, satire, caricature and pastiche, (ii) commenting on current events and (iii) quotation of copyright works.

The precise meaning of "(i) parody, satire, caricature and pastiche" is not defined and the use of quotation would have to be no more than what is required by the specific purpose for which it is used in order to facilitate the expression of opinions.

Request for Views on Additional Issues

The Government is also inviting views on the following propositions:

1. Hong Kong should continue to maintain the exhaustive approach to copyright exceptions;
2. Hong Kong should not introduce provisions to the CO to restrict the use of contracts that override statutory copyright exceptions;
3. Hong Kong should not introduce specific provisions to the CO to tackle illicit streaming devices; and
4. Hong Kong should not introduce a copyright-specific judicial site blocking mechanism to the CO.

Importantly, the Consultation Paper acknowledges that this is just the beginning of a much needed amendment exercise, fully recognising that more work needs to be done. In this regard, emerging issues such as (i) the extension of copyright terms of protection, (ii) the introduction of specific copyright exceptions for text and data mining and (iii) AI and copyright will be addressed in the future.

Limitations

Unfortunately, the Government has taken the view that no copyright-specific statutory provisions for site blocking injunctions are necessary in Hong Kong. This is because the current High Court Ordinance already provides a mechanism for seeking injunctions against online copyright infringements. This may be the case, however, obtaining an injunction to control access to piracy websites under the court's general power to grant injunctions can be time-consuming and costly. In contrast, the UK, Australia and Singapore have enacted specific express provisions in their copyright legislations to empower courts to grant site blocking orders. To illustrate, in the UK, the English High Court and the Scottish Court of Session are empowered to grant an injunction against a service provider if it has actual knowledge of another person using its service to infringe copyright. The fact that there are no reported cases in which Hong Kong courts have ordered OSPs to block websites in copyright infringement cases despite rampant digital piracy is perhaps an indication that copyright-specific judicial site blocking provisions should be introduced in the CO.

Conclusion

If the amendments contemplated under the Consultation Paper are implemented, Hong Kong will be in a better position to deal with copyright infringement in the digital environment and these amendments are key to developing Hong Kong as a regional intellectual property trading centre. The inclusion of additional copyright exceptions is important to protect freedom of speech, particularly for common forms of expression such as parody. Hong Kong's current copyright laws are outdated and these amendments are much needed to modernise Hong Kong's copyright regime.

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

HONG KONG

Arbitration

Hong Kong Courts Continue to Take a Pro-Arbitration Approach

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

Jacqueline Tsang, Associate
Mayer Brown, Hong Kong

In the recent case of *Gurkhas Construction Limited v. Craft Façade Tech (Hong Kong) Company Limited* [2021] HKDC 1166, the District Court of Hong Kong once again demonstrated the judiciary's commitment to enforcing an upholding an arbitration clause in a contract, in this case over a subsequent agreement containing non-exclusive jurisdiction clause in favour of the Hong Kong courts.

Facts of the Case

The plaintiff was a company which supplied labour to the defendant, a building contractor, for a construction project. The defendant failed to pay to the plaintiff amounts due under four Purchase Orders ("**POs**"). In the general terms and conditions of the POs, an arbitration clause stated that any dispute arising in connection with the POs shall be referred to arbitration (the "**Arbitration Clause**").

The plaintiff alleged that the parties subsequently reached a settlement of the defendant's debt under the POs, and signed a letter dated 6 April 2020 (the "**April Letter**") setting out the settlement terms, under which the defendant agreed to pay the total outstanding amounts under the POs by a stipulated deadline (the "**Purported Settlement Agreement**").

The April Letter contained a jurisdiction clause which provided that "*This settlement shall be governed by and construed in accordance with the laws of Hong Kong Special Administrative Region and the parties to this settlement hereby irrevocably undertake to submit themselves to the non-exclusive jurisdiction of the courts of Hong Kong Special Administrative Region to resolve any dispute arising out of or in connection with this settlement.*" (the "**Jurisdiction Clause**").

As the defendant failed to pay the outstanding amount agreed under the April Letter, the plaintiff brought an action against the defendant in the District Court for the recovery of the amounts due under the Purported Settlement Agreement.

Stay of Proceedings in Favour of Arbitration

The defendant then made an interlocutory application for an order for court proceedings to be stayed on the basis that the correct jurisdiction for the dispute should be arbitration (the "**Stay Application**").

Whilst the defendant acknowledged that it signed the April Letter, the defendant's case was that there was no binding settlement agreement between the parties. Since the parties' contractual relationship was governed by the POs which incorporated the Arbitration Clause, the plaintiff's claims in this action were subject to the Arbitration Clause. Therefore, it argued that the Court should stay the current proceedings and refer the matter to arbitration.

The defendant further argued that even if the Purported Settlement Agreement was binding, the Jurisdiction Clause did not amount to a sufficiently clear and unequivocal waiver of the Arbitration Clause in the POs. Therefore, the Arbitration Clause is still applicable and any dispute over the defendant's debt under the POs should be referred to arbitration. If a stay of proceedings was not granted by the Court, then there should be two sets of proceedings - one for the dispute over the defendant's debt under the POs in arbitration and the other relating to the dispute over the Purported Settlement Agreement in the District Court.

Decision of the Stay Application and the Four Stage Test

The Court considered the following questions which were set out in the case of *Tommy CP Sze & Co v Li & Fung (Trading) Ltd & Others* [2003] 1 HKC 418, namely:

1. Is the clause in question an arbitration agreement?
2. Is the arbitration agreement null and void, inoperative or incapable of being performed?
3. Is there in reality a dispute or difference between the parties?
4. Is the dispute or difference within the ambit of the agreement between the parties?

If the answers to questions (1), (3) and (4) are "yes" and the answer to question (2) is "no", the Court should stay the action and refer the matter to arbitration.

In this case, the Court found with relative ease that the answers to questions (1) and (3) were "yes", and the answer to question (2) was "no". The fourth question was the most contentious and was considered more thoroughly by the District Court. The Court found that the Arbitration Clause was wide in scope. The Court further found that irrespective of whether there was a binding settlement agreement, the plaintiff's claims regarding the Purported Settlement Agreement and the April Letter were claims which arise out of or are in connection with the POs. Therefore, the Arbitration Clause applies and the claims at hand should be referred to arbitration.

It is noteworthy that the Court adopted the presumption in favour of one-stop adjudication when construing the Arbitration Clause - i.e. the parties as rational businessmen should have intended for all their disputes arising out of their relationship to be decided by the same tribunal and there should not be two set of proceedings, unless there is an express agreement to the contrary. Taking this into account , the Court found that the Jurisdiction Clause (a non-exclusive jurisdiction clause) was not an express agreement that all disputes should only be submitted to the Hong Kong courts. The Court therefore held that the parties were still bound by

the Arbitration Clause and granted a stay of the court proceedings in favour of arbitration. This is consistent with Hong Kong courts' recent trend of upholding arbitration agreements over a non-exclusive jurisdiction clause.

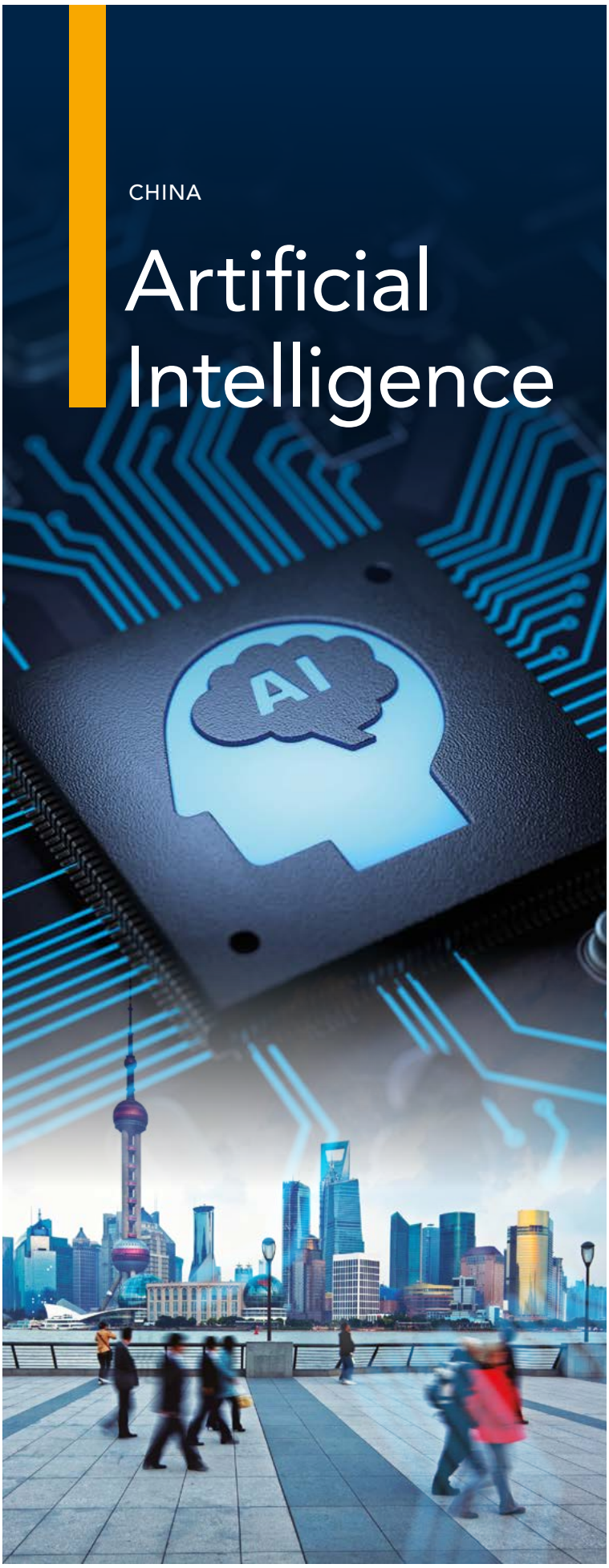
Conclusion

This case once again illustrates the Hong Kong judiciary's pro-arbitration stance and highlights the need for clear language in drafting arbitration and jurisdiction clauses. Had the Purported Settlement Agreement unequivocally waived the Arbitration Clause, the choice of dispute resolution for this dispute may have been different.

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

CHINA

Artificial Intelligence



China Announces Three-Year Plan to Strengthen the Management of Algorithms

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

Cheng Hau Yeo, Associate
Mayer Brown, Singapore

On 29 September 2021, the Cyberspace Administration of China ("**CAC**") issued the "Guiding Opinions on Management of Internet Information Services Algorithmic" ("**Guidelines**"),[2] which is a three-year plan to strengthen the management of algorithms in the Internet industry in China. The Guidelines were endorsed by eight other regulators, including the National Radio and Television Administration, the Propaganda Department of the Communist Party, the State Administration for Market Regulation, the Ministry of Education, the Ministry of Culture and Tourism, the Ministry of Science and Technology, the Ministry of Public Security, and the Ministry of Industry and Information Technology.

The release of the Guidelines follows an earlier announcement on 27 August 2021 on the release of the draft Regulations on the Management of Internet Information Services Algorithmic Recommendation ("**Regulations**").[3] Both the Guidelines and draft Regulations outline the CAC's goal in fostering "positive energy" and "social order" in the cyberspace, as well as tightening its control over the technology industry.

2 关于印发《关于加强互联网信息服务算法综合治理的指导意见》的通知-中共中央网络安全和信息化委员会办公室 (cac.gov.cn)

3 国家互联网信息办公室关于《互联网信息服务算法推荐管理规定（征求意见稿）》公开征求意见的通知-中共中央网络安全和信息化委员会办公室 (cac.gov.cn)

Further details of the draft Regulations can be found in our earlier article at: https://www.mayerbrown.com/en/perspectives-events/publications/2021/09/asia-ip-tmt-quarterly-review-third-quarter-2021.

Much like the draft Regulations, the Guidelines are enthused by fundamental principles such as promoting "positive energy", "accountability", "socialism", "fairness", "transparency" and "social order". The Guidelines also focus on safety assessments of algorithms, record-keeping, and include provisions whose effect is to clamp down on illegal activities which were previously addressed in the draft Regulations.

Algorithm Security Governance Mechanism

The Guidelines propose implementing an algorithm security governance mechanism which involves multiple stakeholders including the government, enterprises, industry organisations and Internet users. Some of the proposals featured in relation to this mechanism are set out below:

1. Companies must develop an internal review mechanism for their algorithms to ensure that they are being used safely, and to respond to any security emergencies. They should be held responsible for the consequences of such occurrences.
2. Netizens are encouraged to report to government departments any suspicious behaviour detected from their use of algorithms.
3. Internet service providers should monitor the latest developments, welcome professional expert terms in the field, and attract investments to promote the responsible development of algorithms.

Algorithm Regulatory System

The Guidelines also propose certain measures which aim to build an algorithm regulatory system which encourages the safe use of algorithms. For example:

1. Companies must actively monitor safety risks and anticipate and prevent potential unfair outcomes such as misinformation, social injustice, and immorality.
2. An algorithm filing system should be established which allows for the filing of algorithms based on different algorithm classifications.
3. Penalties will be introduced for any violations of laws and regulations discovered through the monitoring, evaluation or filing of algorithms, and focus on maintaining the security of algorithms used in Internet information services.

Development of Proper Standards and Values

Finally, the Guidelines also seek to introduce a framework for the responsible use of algorithms. For example:

1. Algorithms must ensure that they promote responsible political points of view, discourse and value judgments. The distribution of information through algorithms should be standardised and carried out in an orderly fashion and algorithms should generally be put to good use.
2. The integration of algorithms into society and economy should be carried out in a manner which protects intellectual property rights, and encourages domestic innovation and the competitiveness of algorithms.
3. The risk of algorithm abuse should be prevented by maintaining order in the cyberspace and social order, and preventing the use of algorithms todistort public opinion, suppress competition or infringe the rights and interests of netizens.

These Guidelines form part of China's broader cybersecurity arsenal. The 2017 Cybersecurity Law was wide in scope, covering internet security, protection of sensitive and personal information, and cyberspace sovereignty, amongst others. The Data Security Law which took effect on 1 September 2021 regulate the collection and use of all data, with a specific focus on important and national core data. The Personal Information Protection Law, which took effect on 1 November 2021, specifically regulates the collection and handling of personal information. Accordingly, these Guidelines represents a more specific area of cybersecurity focusing in particular on the use of algorithms.

Global Significance

The Guidelines (together with the draft Regulations) stand out as the world's first nationwide, comprehensive guiding opinion and rules on algorithms. While areas such as big data and technology secrets are becoming increasingly regulated around the world, the specific area of algorithms have remained largely untouched. Given the increasing use and importance of algorithms in affecting users' thoughts and behaviours, as well as the cyberspace becoming a frequent battleground between states, similar controls may soon be rolled out in other jurisdictions across the world.

Takeaways

The Guidelines provide a useful regulatory basis for local Chinese regulators in relation to this relatively untouched area of cybersecurity. Further detailed regulations in this space may be on the horizon and companies that use algorithms during the course of their business in China should carry out internal reviews to ensure that their algorithms comply with the Guidelines.

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

CHINA

Artificial Intelligence

Humans Versus Robots: China Releases Ethical Guidelines on the Use of Artificial Intelligence

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

Cheng Hau Yeo, Associate
Mayer Brown, Singapore

On 25 September 2021, the Ministry of Science and Technology ("**MST**") released China's first set of detailed ethical guidelines on artificial intelligence ("**AI**"), namely the "Ethical Code on a New Generation of Artificial Intelligence" ("**Code**")[4]. While the Code represents the first of its kind in the country, it forms part of Beijing's long-standing push for technological dominance and global leadership in this field. Key to the Code are provisions placing ultimate responsibility for use of AI, on humans.

Background

The committee that drafted the Code, "New Generation of Artificial Intelligence Governance Committee", was established by the MST in February 2019. It previously published a preliminary set of AI governance guidelines in June 2019[5], which was comparatively less detailed than the Code. The previous guidelines laid the

4 《新一代人工智能伦理规范》发布 - 中华人民共和国科学技术部 (most.gov.cn)

5 Chinese original: Perma | 发展负责任的人工智能: 新一代人工智能治理原则发布
English translation: Perma | Translation: Chinese Expert Group Offers 'Governance Principles' for 'Responsible AI'

groundwork for the MST to pursue its commitment to a framework that sees AI as being "reliable", "sustainable", as well as "harmonious for a common destiny for AI and humans". In particular, the guidelines referenced eight key principles:

1. Harmony and friendliness
2. Fairness and justice
3. Inclusiveness and sharing
4. Respect for privacy
5. Security and control
6. Shared responsibility
7. Open cooperation
8. Agile governance

Many of the values enshrined in the 2019 guidelines have been replicated in the Code, such as values relating to the elimination of bias and discrimination in data analysis and algorithm design, and protecting individuals' right to notification and consent.

The Code

Compared to the 2019 guidelines, the Code introduces more specific requirements for the use and development of AI, which aim to ensure that AI is "controllable by" and "accountable to" humans.

The key regulations focus on:

1. Adhering to market regulations on trading and fair competition, and refraining from engaging in anti-competitive behaviour such as data monopoly and intellectual property infringement;
2. Preventing threats to personal safety, financial security and privacy caused by defective AI products;
3. Protecting users' rights by notifying them when AI technology is used in the provision of goods and services, including the precise functions of such AI, and allowing them to refuse its application;
4. Strengthening emergency measures and compensation mechanism;
5. Promoting the good faith development of AI;
6. Prohibiting the use of any AI technology which undermines national security, rule of law, morality, public safety, and product safety.

AI Regulation and Guidelines in Other Jurisdictions

Similar regulations or guidelines relating to the ethical use of AI have also been published or proposed in various other major jurisdictions.

For example, on 21 April 2021, the European Commission proposed to lay down a set of harmonised rules on artificial intelligence ("**Artificial Intelligence Act**")[6]. The Artificial Intelligence Act employs a risk-based approach and categorises AI systems according to the risks imposed to individuals. Corresponding compliance requirements will be applied to different risk categories, which contain a higher degree of specificity when compared to the Code. Notably, the Artificial Intelligence Act proposes a fine of up to 6% of the business' global annual turnover, which is higher than the maximum level of fines imposed under the General Data Protection Regulation (4% of global annual turnover) or the Personal Information Protection Law in China (5% of annual turnover, albeit unclear whether regional or global).

In Asia, the Ministry of Economy, Trade and Industry in Japan released a set of draft AI governance guidelines for public comments earlier this year. Separately, in 2020, the Personal Data Protection Commission in Singapore released the second edition of the Model AI Governance Framework which provides sector-specific guidance and illustrations on how to determine the level of human involvement in AI-augmented decision-making, as well as updating companies' existing internal governance structures to cater for the risks and responsibilities relating to AI. In Hong Kong, the Office of the Privacy Commissioner for Personal Data published the "Guidance on the Ethical Development and Use of Artificial Intelligence" on 18 August 2021 to assist organisations in developing and using AI in a responsible and ethical manner that is in compliant with their obligations under the Personal Data (Privacy) Ordinance (Cap. 486). Unlike the Artificial Intelligence Act proposed in the EU, the guidelines released in Japan, Singapore and Hong Kong are not legally binding and serve as a "best practices" guide for organisations to follow. For further details on these guidelines, you may refer to our previous article "*Using AI Responsibly: PCPD publishes Guidance*

6 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

on Ethical Development and Use of AI" at: https://www.mayerbrown.com/en/perspectives-events/publications/2021/09/asia-ip-tmt-quarterly-review-third-quarter-2021.

Takeaways

Although not specifically mentioned in the Code, it is anticipated that the Code will only apply to non-government entities. This practice would be in line with the nation's biometric surveillance network which was used to supplement the Social Credit System.

The Code provides welcome guidance to organisations adopting AI technology as part of their business operations. Although some of its provisions remain ambiguous, it nonetheless signifies a step in the right direction when it comes to the use of AI and the protection of user rights. The Code underscores China's ambition to become a world leader in AI by 2030, as announced in 2017, with these guidelines helping to create a robust and accountable framework within which Chinese AI innovation may flourish.

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

China Issues Draft Network Security Management Regulations

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

Cheng Hau Yeo, Associate
Mayer Brown, Singapore

Introduction

On 14 November 2021, two weeks after the Personal Information Protection Law ("**PIPL**") came into effect and more than two months after the Data Security Law ("**DSL**") was implemented, the Cyberspace Administration of China ("**CAC**") released the draft Network Data Security Management Regulations ("**Draft Regulations**") which provide further details and clarifications on various obligations imposed under the PIPL and DSL, as well as the Cybersecurity Law of 2016 ("**CSL**"). The Draft Regulations are open for public comments until 13 December 2021.

We set out below a summary of the key provisions under the Draft Regulations.

Extraterritorial Effect

Article 2 of the Draft Regulations extends the application of the regulations to any data processing activities that: (i) serve the purpose of providing goods and services within China; (ii) analyse and evaluate the behaviour of Chinese individuals or organisations; or (iii) involve "important data'. The extra-territorial reach is consistent approach under PIPL. However, questions have been raised over whether such extra-territorial reach will apply solely in a business-to-consumer context or whether data processing

activities in a business-to-business context will also be covered.

Corporate Compliance

In July 2021, additional requirements relating to cybersecurity reviews were imposed on Chinese companies processing personal data of over one million individuals and wishing to list publicly outside of China. It was widely recognised that the move was triggered by Didi Chuxing's listing in New York despite not having received full clearance from the CAC, which immediately led to a full-scale cybersecurity investigation into two other Chinese companies that had listed in New York shortly before, namely Full Truck Alliance and Kanzhun / Boss Zhipin.

The Draft Regulations extend the cybersecurity review requirement to data controllers seeking to carry out an IPO in Hong Kong that may potentially affect national security,[7] although the requirements remain less stringent compared to organisations applying to list elsewhere. In short, the Draft Regulations may have an impact on potential listings on the Hong Kong Stock Exchange.

With regard to mergers and acquisitions, the Draft Regulations build upon the PIPL's requirement for buyers to continue fulfilling the existing data security duties of any acquired entity, and require the parties to notify the municipal-level authorities where the merger, acquisition or corporate re-organisation involves important data or personal data relating to more than 1 million data subjects.[8]

Important Data and "Large Volume" Data Processors

The Draft Regulations establish a data classification system based on the potential impact on national security and interests[9] and provides a definition of "important data" as data that, once tampered with, may cause harm to national security or public interests,[10] and also contains a non-exhaustive list of the types of data that will be considered as important data, such as undisclosed government-related data, production and operational data in key industries and fields such as manufacturing, telecommunications, energy, transportation, water utilities, finance, defence technology, taxation, customs, and so on. All organisations are required to classify their China data as either "general", "important" or "core" data. However, "data" under the Draft Regulations refers to only "network data" (i.e. data in electronic form). Therefore, the scope of applicability of the Draft Regulations is narrower than that of the DSL or PIPL (which are medium agnostic) and closer to the CSL (which applies only to electronic data).

The Draft Regulations impose various obligations on organisations that process "important" or "core" data. In addition, organisations that process personal data of over one million individuals will also be subject to the same requirements imposed on organisations processing important data under the Draft Regulations.[11] These include: (i) appointing a data protection officer and establishing a data security management agency (to be led by the data protection officer); (ii) filing certain specified information with the relevant local network information government department within 15 working days after identifying any important data being collected; (iii) formulating a data security training plan and carrying out data security training for employees annually; (iv) conducting annual data security assessments (by the organisations themselves or by a third party data security agency), with the security assessment reports to be submitted to the authorities before January 31 of each year; (v) obtaining prior consent from the relevant department of the local city government for sharing or trading data (or engaging a third party data processor to process such data) whether within or outside of China.[12]

Separately, under the Draft Regulations, critical information infrastructure operators ("**CII operators**") are now required to undergo and pass a

7 Article 13 of Draft Regulations
8 Article 14 of Draft Regulations
9 Article 5 of Draft Regulations
10 Article 73 of Draft Regulations
11 Article 26 of Draft Regulation
12 Chapter 4 of Draft Regulations

security assessment conducted by the CAC when procuring any cloud computing services.[13] This is similar to the draft Cybersecurity Review Measures last issued in July 2021 which require CII operators to apply for a security review to be conducted by the CAC when they procure network products and services that may impact national security. This requirement will likely have an impact on the decision of CII operators in their procurement of cloud computing services in China (e.g. choosing a service provider based on security standards, choosing a foreign vs. domestic service provider).

General and Cross-Border Data Transfers

Regarding general data transfers, the PIPL currently requires certain specific contractual terms to be put in place for the transfer of personal data to data processors (processing personal data on behalf of the data controller) or for any cross-border data transfers. These terms include the purpose, scope and methods of, and the security measures to be taken for, the processing by the recipient. Under the Draft Regulations, these requirements have been extended to the transfer of data to other data controllers (whether located within or outside of China).[14]

Regarding cross-border data transfers, the PIPL currently sets out certain requirements (such as entering into a standard contract prescribed by the CAC) which must be complied with when transferring any personal data outside of China. The Draft Regulations extend these requirements to encompass all forms of data (not just personal data) that will be transferred outside of China.[15] However, the Draft Regulations also provide a new exception where the data transfer is initiated for the purpose of entering into or fulfilling a contract with the data subject, or where the life, health or property of the data subject is at risk.[16] However, given that such exception was not specified in the PIPL, it is uncertain whether the position under PIPL (that any one of the requirements must be fulfilled, e.g. entering into standard contract, passing regulatory security assessment, obtaining professional certification, etc.) will still apply strictly without exceptions. We expect such differing requirements to be reconciled in the next draft of the regulations.

The Draft Regulations also provide clarity on requirements relating to subsequent offshore transfers of personal data – a point which was previously unclear under the PIPL. In particular, the conditions for such subsequent transfers must be agreed with the data subject in advance and the security protection obligations to be imposed on the data recipients must be notified to the data subject.[17] This may turn out to be fairly restrictive on organisations that regularly carry out intra-group data transfers or engage the data processing services of various offshore subcontractors.

Consent and Notification

The Draft Regulations expand the notification requirements under the PIPL by requiring the data controllers to notify the data subjects of the processing purposes, method, location etc., and categories of personal data being processed by each specific function of a product or service, and to obtain consent from the data subject separately for the processing of his or her personal data by each business function.[18] This mirrors the approach previously recommended by the non-binding Information Security Technology – Personal Information Security Specification last updated in 2020.

In addition, the Draft Regulations also require additional information to be disclosed by the data controllers to data subjects such as information relating to third-party plug-ins and other access points incorporated in their websites and apps, information relating to the personal data security risks and protection measures taken, and details on the complaint channels for reporting any personal data security issues.[19]

13 Article 34 of Draft Regulations
14 Article 12 of Draft Regulations
15 Article 35 of Draft Regulations
16 *Ibid*
17 Article 39(9) of Draft Regulations
18 Article 20(1) of Draft Regulations
19 Article 20(4) of Draft Regulations

Data Breach Notification

Under the Draft Regulations, a data controller is required to report a data breach incident to the affected parties (e.g. individuals and/or organisations) where the data breach incident causes harm to such individuals or organisations.[20] This is consistent with the PIPL (under which data controllers can elect not to notify affected data subjects if they determine that they have taken measures which effectively prevent the data subjects from suffering any harm from the data breach incident), although it is unclear how this requirement will apply in practice with the other breach notification requirements imposed under the DSL and CSL.

Where required, such data breach notification has to be made to the affected parties within 3 working days and the notification has to include details of the data breach incident, the risks and potential impact of harm, and the remedial measures that have been taken. We note that this deadline is similar to the 72-hour breach notification deadline imposed under the EU's GDPR.[21]

For serious security incidents (i.e. leakage, destruction, or loss of important data or personal data of more than 100,000 people), the data controller is required to: (i) submit an initial report (containing details of the volume and type of data affected, potential impact and remedial measures that have been or are planned to be taken) to the authorities within 8 hours of the occurrence of the incident; and (ii) submit an investigation and assessment report (containing details of the cause of the incident, impact of the incident, handling of the incident and remedial measures taken to prevent the reoccurrence of a similar incident) to the authorities within 5 working days after the incident has been handled.[22]

The breach notification requirements imposed under the Draft Regulations appear to be fairly strict and many organisations may find it challenging to comply with the requirements and in particular, the tight notification deadlines.

Takeaways

The Draft Regulations provide much-needed clarity on some of the obligations imposed under the DSL, PIPL, and CSL, although some uncertainties still remain. While no timeline for the finalisation and enactment of the Draft Regulations has been given, businesses should start making preparations for compliance with the Draft Regulations, given that some of the proposed obligations appear to be fairly challenging and may require some time to ensure compliance. There is a possibility that the Draft Regulations may be rapidly passed into law with only a short period of time before they come into effect (and no further grace period), leaving organisations with little time to get their affairs in order. In addition, organisations should also continue to monitor the data privacy and cybersecurity legal landscape in China for any further developments or new updates.

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

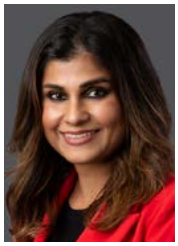
20 Article 11 of Draft Regulations

21 *Ibid*

22 *Ibid*

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

Cheng Hau Yeo
Associate
+65 6922 2245
chenghau.yeo@mayerbrown.com

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

This Mayer Brown publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek legal advice before taking any action with respect to the matters discussed herein.

Mayer Brown is a global services provider comprising associated legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England), Mayer Brown (a Hong Kong partnership) and Tauil & Chequer Advogados (a Brazilian law partnership) (collectively the "Mayer Brown Practices") and non-legal service providers, which provide consultancy services (the "Mayer Brown Consultancies"). The Mayer Brown Practices and Mayer Brown Consultancies are established in various jurisdictions and may be a legal person or a partnership. Details of the individual Mayer Brown Practices and Mayer Brown Consultancies can be found in the Legal Notices section of our website. "Mayer Brown" and the Mayer Brown logo are the trademarks of Mayer Brown.

© 2021 Mayer Brown. All rights reserved.

Attorney Advertising. Prior results do not guarantee a similar outcome.

Americas | Asia | Europe | Middle East

mayerbrown.com