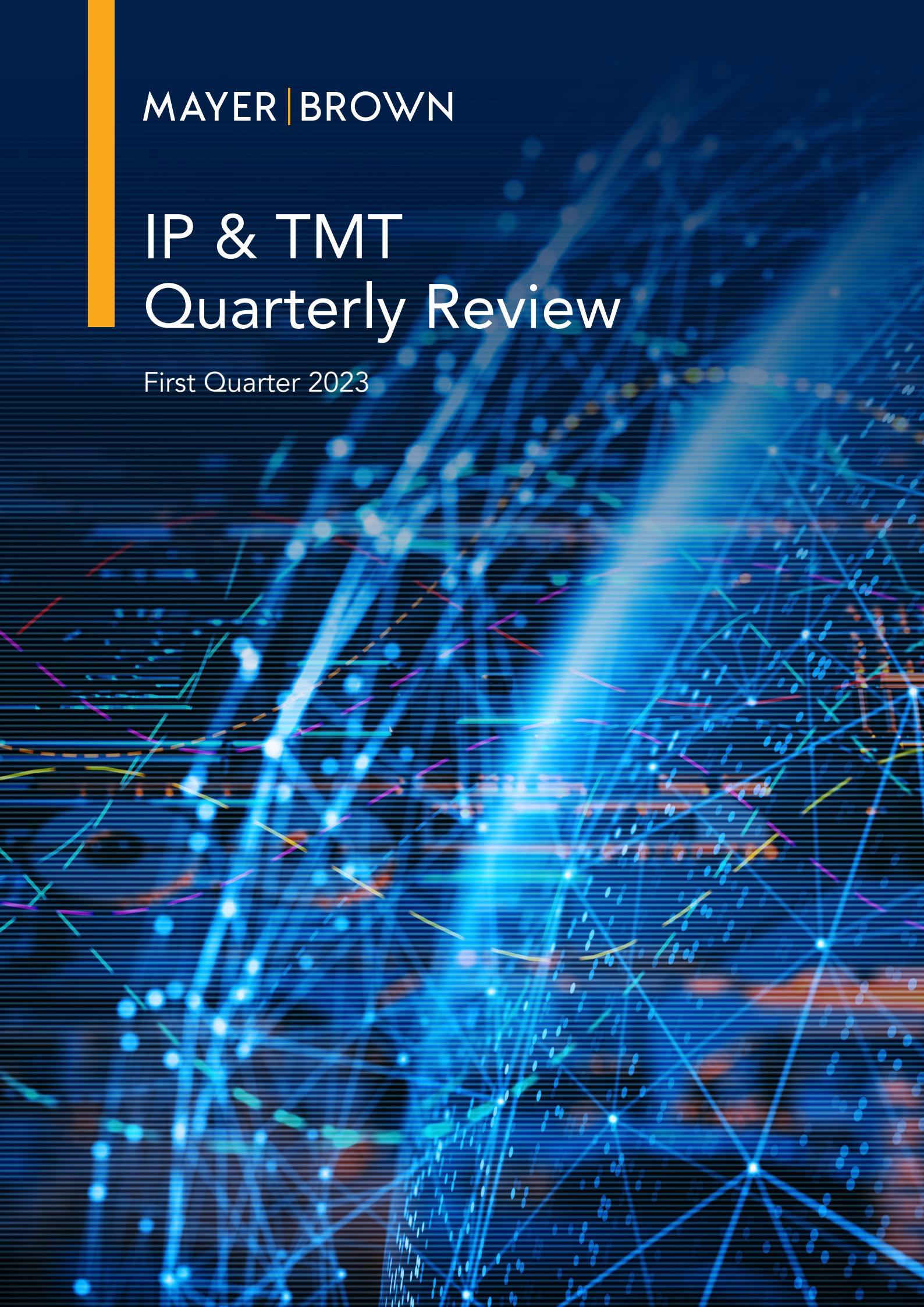
MAYER | BROWN

IP & TMT Quarterly Review

First Quarter 2023



Contents

2 Data Privacy
China

9 Intellectual Property
China

13 Intellectual Property
Hong Kong

18 Media
Hong Kong

21

China: The "Gold" Standard – Long-Anticipated Standard Contract under Personal Information Protection Law Finalised

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

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

The Cyberspace Administration of China ("**CAC**") issued the Measures on Standard Contracts for the Export of Personal Information ("**SC Measures**") on 24 February 2023, finalising the hotly-anticipated standard contract for the export of personal information ("**Standard Contract**") under the Personal Information Protection Law ("**PIPL**"). The SC Measures come after more than a year since PIPL was brought in, and almost eight months after the release of the Draft Provisions on Standard Contracts for the Export of Personal Information ("**Draft Standard Contract Provisions**") (see our previous Legal Update on the Draft Standard Contract).

The finalised Standard Contract becomes effective on 1 June 2023, but with a 6-month grace period (until 30 November 2023) for personal information exports which commenced prior to 1 June 2023.[1]

1 Article 13, SC Measures.

Personal information processors[2] ("**data controllers**") eligible to rely on the Standard Contract (see below section on **Application**) are expected to revise their data export processes and procedures within the grace period to comply with the SC Measures and the Standard Contract.

Export of Personal Information – Background

Under Article 38 of the PIPL, there are three mechanisms that data controllers may utilise in order to export personal information outside of the People's Republic of China ("**PRC**"): (i) the Security Assessment; ii) the Certification or iii) the Standard Contract.

The Security Assessment was finalised by the CAC last year and took effect on 1 September 2022, while a revised draft Certification specification was recently released on 8 November 2022 and finalised on 16 December 2022 (see our previous Legal Update on the Security Assessment and Revised Certification Specification).

The requirements under the Security Assessment are onerous and mandatory for data controllers that process or export personal information over a certain threshold, or, are deemed to be critical information infrastructure operators, while the Certification appears to be designed mainly for intra-group transfers.

Accordingly, the Standard Contract is likely to be the most widely used mechanism for exporting data out of the PRC. In this legal update, we look at the key provisions of the finalised Standard Contract and the SC Measures.

Application

Under the SC Measures, data controllers must fulfil all the following criteria in order to be able to use Standard Contracts for the export of data. They must be:

1. An entity not classified as a CIIO;
2. Data controllers processing the personal information of less than 1 million data subjects;
3. Data controllers who have exported:
   a. the personal information of less than 100,000 data subjects; or
   b. the sensitive personal information of less than 10,000 data subjects, since January 1 of the previous year; and
4. Also not fall within other circumstances as may be specified by other laws, regulations and rules.

However, the SC Measures now prohibit data controllers from dividing data exports into separate batches to circumvent the Security Assessment.[3] This was previously unaddressed in the Draft Standard Contract Provisions and seemed to be a possible practical solution. The revision ostensibly targets large companies seeking to carry out large data exports through the use of subsidiaries and related companies in a piecemeal fashion, in order to avoid the Security Assessment. Nevertheless, it is unclear in what circumstances a division of personal information would be prohibited and what would be considered *bona fide*.

Obligations of Data Controllers

Under the Standard Contract, data controllers are required to notify data subjects of the foreign recipient's name, contract information, purposes and methods of processing, types and retention period of personal information, the methods and procedures for exercising their rights as a data subject and "*other matters*" (*see Exhibit 1 (Instructions for the Export of Personal Information*")[4]. Where the export involves sensitive personal information, the necessity and the impact of such export on the rights and interests of the data subjects must also be notified to them.

The primary basis for the collection and processing of personal information under the PIPL is the data subject's consent.[5] However, data controllers are

2 The PIPL uses the term "personal information processor" (not to be confused with the commonly used term "data processor") to refer to "*organizations and individuals that, in personal information processing activities, autonomously decide processing purposes and processing methods*" – this is akin to the concept of a "data controller" under other commonly encountered data protection legislation.

3 Article 4, SC Measures.

4 Article 2(2), Standard Contract.

5 Article 13, PIPL.

required to obtain separate consent (e.g. unbundled consent) from data subjects in specific scenarios (e.g. export of personal information). The Standard Contract highlights one such scenario where separate, unbundled consent is required for the export of personal information, or from parents or guardians for the export of personal information of minors under the age of 14.[6]

Notably, data controllers must also inform data subjects of their third party beneficiary rights (see section on **Data Subject Rights** below), which crystalise if the data subject does not expressly object within 30 days.[7]

As the more "proximate" entity to the CAC, data controller exporters have the de facto burden of ensuring that the foreign recipient's data protection practices are sufficient; under the Standard Contract, data controllers have the burden of making "*reasonable efforts to ensure that the foreign recipient will take the necessary technical and management measures (encryption, anonymisation, de-identification, access control, and other technical and management measures)*".[8] Coupled with the added obligations of responding to inquiries from the Regulatory Authority regarding the processing activities of the foreign recipient,[9] and impact assessment to determine whether the foreign recipient's management, technical measures and capabilities to perform the responsibilities and obligations can ensure the security of exported personal information[10], in effect this would mean a full audit of the practices of the foreign recipient pre-transfer. Such documentary evidence in practice will be gathered to satisfy the Personal Information Protection Impact Assessment ("**PIA**") requirements, and will need to be kept for at least 3 years.

Strict Compliance

The SC Measures also now explicitly provide that the Standard Contract is to be used in its entirety, without deviation, unless otherwise directed by the CAC. In any event, while data controllers may include additional clauses in the Standard Contract (as an exhibit), such clauses should not conflict with the Standard Contract, which should prevail in any case.[11] Companies intending to export data out of the PRC should therefore re-visit their pre-existing documentation used for exporting data out of the PRC (e.g. intra-group data transfer agreements, data processing agreements etc.).

PIA

The SC Measures have retained the requirement for data controllers to carry out a PIA prior to the export of personal information. The PIA is to focus on the following areas:

1. The legality, legitimacy, and necessity of the purpose, scope, and methods of personal information processing by the data controller and foreign recipients;
2. The scale, scope, type, and sensitivity of exported personal information, and the potential risks to the rights and interests in personal information that may arise;
3. The responsibilities and obligations undertaken by the foreign recipient, as well as whether the management, technical measures and capabilities to perform the responsibilities and obligations can ensure the security of exported personal information;
4. The risk that personal information will be altered, destroyed, leaked, lost, transferred, or illegally acquired or used during or after export, and whether channels have been established to safeguard data subjects' rights and interests in their personal information rights;
5. The impact of the policies, laws, and regulations of the foreign recipient's jurisdiction on the performance of a standard contract; and
6. Other matters that may affect the security of personal information exported,

and should be kept for at least 3 years.

Data controllers must submit the completed PIA report together with the executed Standard

6 Article 2(3), Standard Contract.
7 Article 2(4), Standard Contract.
8 Article 2(5), Standard Contract.
9 Article 2(7), Standard Contract.
10 Article 2(8)(iii), Standard Contract.
11 Article 6, SC Measures; Article 9(1), Standard Contract.

Contract to the regulatory authorities within 10 working days of the effective date of the Standard Contract,[12] though this appears to be a procedural formality without any need for regulatory approval, with data controllers being responsible for the "*veracity of documents filed*".[13]

These requirements are consistent with the PIA requirements under the other Security Assessment and Certification data export mechanisms.

Submission of Documents

The SC Measures have retained the requirement for data controllers to submit a new Standard Contract in certain circumstances though the first scenario has been narrowed slightly (dropping changes to the 'quantity' and 'retention period' of personal information). In such an event, the Standard Contract has to be executed again and filed anew with the regulatory authorities:

1. Changes to purpose, scope, type, sensitivity, methods, storage location of exported personal information, and the purposes and methods for which foreign recipients process data, or extend the period of overseas retention of personal information.
2. Changes to the policies, laws or regulations on the protection of personal information in the foreign recipient's jurisdiction that might impact rights and interests in personal information; or
3. Other circumstances that may impact rights and interests in personal information.

However, the SC Measures now allow data controllers to "*supplement [the Standard Contract]*" (i.e. file an addendum) as an alternative to re-filing the entire Standard Contract.

In practice most companies will opt for filing a supplement to the Standard Contract in the event of any of the changes detailed in the first scenario. The second and third scenarios remain tricky given the shifting sands of data protection regulations which will put the onus on data exporters to keep up to date with regulatory and legal changes and make an assessment whether such changes fall within the second scenario. The third scenario is nebulous and difficult to interpret and will likely never be invoked by data exporters but may prove a useful 'stick' for regulators especially if data exports are caught in the cross-fire of geopolitical battles.

The SC Measures now also require data controllers to carry out a new PIA to account for such changes in the scenarios outlined above and file the new PIA alongside the refreshed Standard Contract with the local CAC office. Data controllers should therefore be mindful as to changes to the circumstances in which it exports data since this could require it to prepare and file a new PIA and Standard Contract.

Whistleblowing Provision

Violations of the SC Measures can be brought to the attention of the regulators by any third party (e.g. competitors and disgruntled former employees). Companies that export data out of the PRC should be mindful of this provision which highlights again the importance of compliance and of restricting sensitive discussions on data strategy to the C-suite and or personnel in management roles and on a "need to know" basis.

Additional Obligations for Foreign Recipients

Under the finalised Standard Contract, there are also several new obligations for foreign recipients, including:

1. Obtaining separate consent of data subjects if any personal information is processed beyond the agreed purpose, method of processing and/or type of processing personal information.[14]
2. Obtaining separate consent from parents or other guardians of minors if personal information of a minor under the age of 14 is involved.[15]
3. (For data processor recipients) Returning or deleting personal information if the data processing agreement is ineffective, invalid, revoked or terminated, and providing a written

12 Article 7, SC Measures.

13 Article 8, SC Measures.

14 Article 3(1), SC Measures.

15 ibid.

statement to confirm such actions have been taken.[16]

The Draft Standard Contract previously required foreign recipients to take certain actions in the event of a "data breach". This has now been clarified to mean "*the occurrence or possible occurrence of alteration, destruction, leakage, loss, illegally use, unauthorised provision of or access to the processed personal information*".[17]

Under the SC Measures, where there has been a *possible* alteration, destruction, leakage, loss, illegally use, unauthorised provision of or access to the processed personal information, foreign recipients are required to:[18]

1. Take timely remedial action to mitigate adverse effects on data subjects;
2. Immediately notify the data controller and report to the regulatory authority as required by applicable laws, including the types of personal information affected, remedial actions taken, measures data subjects can take to mitigate damage, and the contact details of the personnel responsible for handling the breach; and
3. Document and retain all relevant evidence of alteration, destruction, leakage, loss, illegally use, unauthorised provision of or access including all remedial actions taken.

Laws and Regulations of the Foreign Recipient's Jurisdiction

The finalised Standard Contract requires both the foreign recipient and exporting data controller to warrant that they have "*exerted a reasonable duty of care*" when signing the Standard Contract, and they are not aware of personal information protection laws or regulations of the country where the foreign recipient is located, which include any provisions authorising public authorities to access personal information, that will impact a foreign recipient's performance of their obligations.[19]

This inclusion of "*reasonable duty of care*" is novel to the finalised Standard Contract, and while it is uncertain what this will entail, seems to suggest that a legal opinion of local counsel (of the foreign recipient jurisdiction) may be required – much like the Transfer Impact Assessments required under the GDPR in the wake of Schrems II.

Notably, this is not a blanket restriction on transfers to countries where public authorities may access personal information, but appears to be a point for data controllers to analyse and assess. This is particularly in light of the new Article 4(6) of the Standard Contract, which requires foreign recipients to immediately notify the data controller in the event that it receives a request from a government department or judicial organ of the country in which it is located; data controllers may have to be wary of foreign jurisdictions that allow public authority access and prohibit notifications made to the exporting data controller. The provision mirrors somewhat data controller obligations under the PIPL[20] and Data Security Law ("**DSL**")[21] that prohibit the provision of personal information stored within mainland PRC to judicial or government bodies of foreign countries without the approval of the PRC regulatory authorities.

The Standard Contract allows a data controller to suspend and eventually terminate the contract in the event there are changes in the laws or mandatory measures in the country where the foreign recipient is located which makes it impossible for the foreign recipient to perform the contract. In short, any conflict of laws issue may result in the termination of the Standard Contract.

Data Subject Rights

Other than the data subject rights accorded to data subjects under the PIPL (e.g. access, restriction, correction, withdrawal of consent, portability, erasure etc.), under the finalised Standard Contract,

16 Article 3(5), SC Measures.
17 Article 3(7), SC Measures.
18 ibid.
19 Article 4(1), SC Measures.
20 Article 41, PIPL.
21 Article 36, DSL.

data subjects are granted third party beneficiary rights that allow them to demand performance of various clauses of the Standard Contract[22] and take action for breach of the Standard Contract. In the event of a dispute, the data subject may lodge a complaint with the regulatory authority[23] or file a lawsuit with an appropriate people's court in accordance with the Civil Procedure Law of the PRC for a breach of the Standard Contract by either or both of the parties.[24]

Since such actions (i.e. complaints and/or a civil claim) will necessarily be premised on the information that is made available to the data subject, given the additional rights that data subjects in the PRC have (e.g. third party beneficiary rights[25], right for data subject to obtain a copy of the SCC from both parties[26], right for data subject to be informed of matters surrounding the export and processing of their personal information[27]), organisations engaged in exporting personal information from the PRC should be mindful of their communications and interactions with data subjects. Data controllers should ensure that they have necessary internal policies and procedures in place to allow them to respond to data subject requests in compliance with the law.

Additional Points of Interest

The ethos of the Standard Contract appears to be that of discouraging the export of personal information given the requirements for personal information to be exported to "the minimum extent required to achieve the purpose of processing"; or the emphasis on disclosure of the personal information to third parties only if there is a "real business need". This is further driven home by the manner in which the eligibility thresholds for the Standard Contract are framed i.e. "*personal information of less than 100,000 data subjects [counted from 1 Jan of the previous year]*", which point to exports of personal information being the exception rather than the norm since data controllers would have to have meticulous record-keeping practices should they wish to comply with the SC Measures.

Volume thresholds. Data controllers should note that the relevant date for determining whether a data controller falls within threshold 3 (i.e. data controllers who have exported personal information of fewer than 100,000 data subjects or sensitive personal information of fewer than 10,000 data subjects) is 1 January of the *previous year*.[28] Data controllers should therefore be mindful of the volume of personal information they export, particularly in the later part of the year (e.g. December) as this determines whether they are likely to be caught within this threshold, which essentially applies to the export of data for a period of up to 2 years. Where the personal information exceeds the stipulated thresholds in the SC Measures, or the data controller is a CIIO, the Security Assessment transfer mechanism 2 will apply. This will require data controllers to be very precise in their record keeping, and limit data exports on a "need to have" basis should they wish to avoid having to undergo a Security Assessment.

Scope of PIA and Exhibit 1 of the Standard Contract. Since changes to the purpose of processing and/or personal information storage location would necessitate a redo of both the PIA and Standard Contract, data controllers may wish to prepare a more expansive PIA and Exhibit 1 (Instructions on the Export of Personal Information) of the Standard Contract.

Audit Rights. The foreign recipient has a broad obligation to provide the data controller with "all information necessary" to allow it to audit the compliance of processing activities.[29] This is accompanied by a corresponding obligation on the data controller provide all such information (including all compliance audit results) to the CAC as may be required by applicable laws.[30] Accordingly, data controllers engaged in pre-existing data transfers

22 Article 5(5), 6(3), Standard Contract.
23 Article 6(3)(i), Standard Contract.
24 Article 6(5), Standard Contract.
25 Article 5(5), Standard Contract.
26 Article 2(9), 3(3), Standard Contract.
27 Article 2(2), Standard Contract
28 Article 4, SC Measures.
29 Article 3(11), Standard Contract.
30 Article 2(11), Standard Contract.

subject to pre-existing agreements should review this documentation to ensure that there are no additional impediments (which may not necessary conflict with the Standard Contract) that may nonetheless impair their ability to comply with the data controller obligations of the Standard Contract.

Unresolved issues. There are still outstanding questions on the practical applicability of the Standard Contract that remain unanswered e.g when would a division of personal data transfers be considered acceptable? How are data controllers exporting personal information expected to practically keep count of personal information exported, and what happens when a data export crosses the eligibility threshold that would require it to undertake a Security Assessment?

Conclusion

While the finalised Standard Contract sheds more light on the compliance requirements data exporters need to undertake, there are still outstanding practical issues that remain, and businesses with a presence in the PRC and those who deal with companies in the PRC ought to commence preparations to ensure they comply with the SC Measures by 30 November 2023.

The 2023 Draft Amendment to the PRC Trade Mark Law: Sweeping Changes to Combat Bad Faith Filings

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

Introduction

Rampant trade mark squatting has been a recurring problem in the PRC, despite the Chinese government's efforts in recent years to crack down on such behaviour through legislative and regulatory measures, such as the amendment to the Trade Mark Law ("**2019 Amendment**") and Several Measures on Regulating Applications to Register Trade Marks ("**Measures**"), both introduced in 2019, the Special Action Plan for Combatting Bad Faith Trade Mark Hijacking and Measures for Collaborative Governance of Violations and Offences in the Patent and Trade Mark Agency Industry in 2021, and more recently, the updated Guidelines for Trade Mark Examination and Review, which came into effect on 1 January 2022 ("**Guidelines**"). Whilst these legislative and regulatory measures introduced welcome changes to the trade mark registration system, including empowering the China National Intellectual Property Administration ("**CNIPA**") to proactively reject applications based on bad faith during substantive examination and the introduction of a blacklist for trade mark agencies that engage or facilitate in bad faith behaviour, ultimately these changes did little to reduce

the number of bad faith filings submitted by squatters.

On 13 January 2023, the CNIPA published a draft amendment of the Trade Mark Law for public consultation until 27 February 2023 ("**2023 Draft Amendment**"). The 2023 Draft Amendment (in its current form) introduces sweeping revisions to the Trade Mark Law, expanding the original 73 articles to 101 articles and substantially amending 45 articles, leaving only 27 existing articles unchanged. The proposed revisions to the Trade Mark Law have been made with the express objective of targeting trade mark squatting and other bad faith filing behaviour. Some of the most significant changes are discussed below.

New Definition of Bad Faith Filing Behaviour

The 2019 Amendment introduced Article 4, which empowered the CNIPA to reject an application filed in "bad faith without intent to use" during substantive examination. What constituted "bad faith without intent to use" had been left undefined, although some guidance was subsequently provided in the Measures and the Guidelines.

The 2023 Draft Amendment includes a newly added Article 22, which specifies four types of filing behaviour for which bad faith will be presumed, together with one catch-all provision:

1. applying to register a large number of trade mark without intent to use, disrupting the order of the trade mark registration system;
2. applying to register trade marks through deception or other improper means;
3. applying to register trade marks that are detrimental to the interests of the State, the public interest, or that have other significant adverse effects;
4. contravening Articles 18 (pre-emptive registration of a well-known trade mark), 19 (pre-emptive registration by agents, representatives or other related parties without authorisation) and 23 (pre-emptive registration obtained by improper means of a trade mark that has attained a certain degree of influence) of the 2023 Draft Amendment, intentionally damaging the legitimate rights or interests of others, or obtaining improper benefits; and
5. engaging in other bad faith filing behaviour.

Mandatory Transfer as an Alternative Remedy to Invalidation

Under the current law, if a brand owner discovers that a third party has registered their mark in bad faith, their only recourse is to apply to invalidate the registration. Under Articles 45 to 47 of the 2023 Draft Amendment, a brand owner can request the transfer of a hijacked trade mark registration (similar to the remedy provided in domain name disputes) as an alternative to invalidation if the mark under dispute is:

1. a pre-emptive registration of the brand owner's well-known trade mark;
2. a pre-emptive registration filed by the brand owner's agents, representatives or other related party without authorisation; or
3. a pre-emptive registration obtained by unfair means of the brand owner's trade mark that has attained a certain degree of influence.

The most important advantage conferred by this new remedy is that it will allow a brand owner to obtain a registration with an early filing date, thus obviating the need for the brand owner to file their own application and deal with intervening third party marks. Under the current regime, even if a brand owner successfully invalidates a copycat registration, their problems may not be over – there could be any number of intervening third party marks that predate the brand owner's own application, and invalidating one copycat registration might only clear the way for the intervening marks.

Administrative Fines and Other Penalties

The 2023 Draft Amendment also includes proposed revisions relating to administrative penalties and fines that may be imposed for bad faith behaviour.

Article 68(4) of the current Trade Mark Law provides that administrative sanctions such as a warning or a fine may be imposed for trade mark applications filed in bad faith. This provision has been amended under Article 67 of the 2023 Draft Amendment,

which provides that, where an application is filed in bad faith in contravention of the new Article 22, administrative warnings or fines up to RMB50,000 may be imposed, and for more serious infractions, fines of up to RMB250,000 may be imposed and any illegal gains may be confiscated.

The 2023 Draft Amendment also provides that, where a brand owner suffers loss due to a bad faith filing under the new Article 22(4), the brand owner may file a civil action against the bad faith filer, and the damages awarded should amount to at least the reasonable expenses incurred by the brand owner to deal with the bad faith filing (the new Article 83). For bad faith filings under the new Article 22(3) (filings that are detrimental to the interests of the State or the public interest), the procuratorate may also take court action against the bad faith filer.

New Obligations to Show Use

As trade mark filing fees in the PRC are relatively low, trade mark squatters will often file large numbers of trade marks in the hopes of attracting potential buyers at a later date, with no intention of actively using or maintaining the marks in the meantime. To target such behaviour, new obligations to show use have been included in the 2023 Draft Amendment. Article 5 of the 2023 Draft Amendment expressly states that a party should only apply to register a trade mark that it uses or undertakes to use the mark on its goods or services. The new Article 61 of the 2023 Draft Amendment goes further and requires registrants to file a declaration of use every five years after registration in order to maintain their trade mark registrations.

The 2023 Draft Amendment represents a departure from the current regime with regard to use – under the current law, a registrant is not required to prove use of their mark unless a third party tries to cancel the registration on the basis of non-use. The new Article 61 imposes a positive obligation on registrants show use every five years to prevent their registrations from being cancelled by the CNIPA.

Restrictions on Repeated Filings

A common issue encountered by brand owners when dealing with bad faith filers is repeated filings. A brand owner will successfully oppose, invalidate or cancel a copycat mark only to discover that the bad faith filer has refiled one or more applications for the same mark. The 2023 Draft Amendment introduces new restrictions on repeated filings of a mark for the same goods / services. Article 14 of the 2023 Draft Amendment provides that, subject to other provisions, a party may only hold one registration for a mark covering the same goods or services. Article 21 of the 2023 Draft Amendment further provides that, where a party's mark has been deregistered, cancelled or invalidated, the same party may not refile a mark for the same goods / services within one year. This prohibition is subject to a number of exceptions, such as, amongst other circumstances, in cases where an earlier registration was removed for failure to renew or failure to defend a non-use cancellation action, provided such failure was for reasons outside the applicant's control, or failure to file a declaration of use provided the mark has been in actual use.

New Grounds for Cancellation

Under the current law, a party may apply to cancel another party's trade mark registration on the basis of non-use for a consecutive three-year period, or if the trade mark has become generic in respect of the designated goods or services. Article 49 of the 2023 Draft Amendment introduces several additional grounds for cancellation, including for example, cases where use of the registered mark causes confusion amongst the relevant public in respect of the quality or other characteristics of the relevant goods or their place of origin; or where use or the exercise of the exclusive rights conferred by a registered mark will cause serious harm to the public interest and have significant adverse effects. Article 49 also provides that in certain circumstances (such as where there is serious harm to the public interest), the CNIPA may make an ex officio decision to cancel a registered mark.

Procedural Changes

Some of the proposed revisions in the 2023 Draft Amendment are intended to streamline and expedite the trade mark registration process. Article 36 of the 2023 Draft Amendment shortens the opposition period from three months to two months. The opposition process will now also be shortened – under the current regime, an opponent is unable to contest an unfavourable opposition decision, but an applicant whose mark has been successfully opposed may contest the decision by filing a review (and if the review is unsuccessful, further contest the decision by filing a court appeal). Article 39 of the 2023 Draft Amendment removes the applicant's right to file a review – an applicant unhappy with an opposition decision will need to appeal to the courts.

Online Use of Trade Marks

The 2023 Draft Amendment also addresses the use of trade marks online. For example, Article 59 expressly includes use on the internet as a valid form of trade mark use; Article 72 provides that unauthorised use in e-commerce of a mark identical or similar to another party's registered trade mark and will likely mislead the public may constitute trade mark infringement.

Conclusion

The 2023 Draft Amendment would, if enacted, result in the substantial changes to the current trade mark registration regime. The introduction of a positive obligation to submit regular declarations of use in order to maintain a registration should help remove a significant number of registrations filed by trade mark squatters, and reduce the need for brand owners to file non-use cancellation actions against unused marks. On the flip side, the new obligation will increase the administrative burden and maintenance costs for legitimate trade mark owners. The restrictions on repeated filings for the same mark should also deter bad faith filers from repeatedly refiling copycat marks, although it could also prevent brand owners from refiling marks for legitimate reasons – the latter issue could to addressed by further elaborating on the circumstances in which repeated filings may be allowed.

Given the extent of the proposed changes, it will be interesting to see how many of the draft amendments will ultimately be adopted. It seems likely that at least some of the proposals will be substantially altered or deleted before enactment.

*The author would like to thank **Sabrina Chow**, Seconded Trainee at Mayer Brown, for her assistance with this article.*

HONG KONG

Intellectual Property

Sailing Into Safe Harbours: Code of Practice for Online Service Providers to Limit Liability for Copyright Infringement

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

Grace Wong, Associate
Mayer Brown, Hong Kong

Introduction

The Copyright (Amendment) Ordinance 2022 will come into operation on 1 May 2023 and bring long-awaited updates to Hong Kong's Copyright Ordinance (Cap. 528) (the "**Ordinance**").[31] We have discussed the key amendments in a previous article "*The Beginning of a New Chapter: Hong Kong's Copyright (Amendment) Bill 2022 is Gazetted*" in our IP & TMT Quarterly Review (Second Quarter 2022).

One of the key amendments is the introduction of safe harbour provisions that limit the liability of Online Service Providers ("**OSP**") for copyright infringement occurring on their platforms.[32] Whilst the conditions for invoking the safe harbour provisions will be listed in the Ordinance, the practical guidelines and procedure of what an OSP should do upon receiving a notice of alleged infringement ("**Notice**") are set out in a voluntary Code of Practice ("**Code**").[33]

31 Original text can be found at Copyright (Amendment) Ordinance 2022.

32 New Part II, Division IIIA of the Ordinance.

33 Original text can be found at Copyright Protection in the Digital Environment--Code of Practice.

The Code of Practice, published by the Secretary for Commerce and Economic Development in February 2023, is based on a draft version formulated in 2012 when the Government's attempted to amend the Ordinance.

As a follow-up to our last article, we examine the "notice and notice" and "notice and takedown" systems set out in the Code.

Safe Harbour Provisions

An OSP will not be liable for damages or other pecuniary remedy for copyright infringement caused by users on their platforms, if all of the conditions below are met:[34]

1. The OSP has taken reasonable steps to limit or stop the infringement as soon as practicable after receiving a Notice, becoming aware that the infringement has occurred, or becoming aware of the facts or circumstances that would lead inevitably to the conclusion that infringement had occurred;
2. The OSP has not received, and is not receiving, any financial benefit directly attributable to the infringement;
3. The OSP accommodates and does not interfere with the standard technical measures that are used by copyright owners to identify or protect their copyright works; and
4. The OSP designates an agent to receive the Notices and supplies the agent's name and contact details on its service.

Related provisions include, for example, the form and procedure of submitting a Notice, what OSPs should do after receiving the Notice or becoming aware of an infringement, and the form and procedure for users to submit a counter notice ("**Counter Notice**") to contest the complaint.[35]

Whilst it is voluntary for OSPs to comply with the Code once they receive a Notice, they will be treated as having taken reasonable steps to limit or stop the infringement in question, as required in condition (1) above, if they have fully complied with the Code.[36] Non-compliance with the Code does not disqualify an OSP from invoking the safe harbour provisions; however, it will need to demonstrate to the Court what reasonable steps it has taken to satisfy condition (1).[37]

"Notice and Notice" or "Notice and Takedown"

An OSP is defined as a person who, by means of electronic equipment and/or a network, provides or operates facilities for any online services.[38] The Code distinguishes between three types of OSPs: (i) OSPs which store materials on their platforms; (ii) OSPs which use information location tools[39] to link or refer to online materials; and (iii) OSPs which only transmit, route or provide connections for digital online communications.

The first two types of OSPs are subject to a "notice and takedown" system. However, a key distinction is that only the first type (i.e. OSPs which store materials on their platforms) may need to reinstate the allegedly infringing material which it had taken down, if (1) it receives a Counter Notice from the user disputing the complaint, and if (2) the complainant does not commence Court proceedings in Hong Kong against the alleged infringement.[40] As for the third type of OSPs, they are subject to a "notice and notice" system as they do not have control over the allegedly infringing material (or the hyperlink or reference to such material).

An overview of the types of OSPs, subject matters of the complaints, and the steps to be taken by the OSPs under the different systems, is shown on the next page.

34 New section 88B of the Ordinance.

35 New sections 88C to 88J of the Ordinance.

36 New sections 88B(3) and 88I of the Ordinance.

37 Paragraph 1.4 of the Code.

38 New sections 65A(2) and 88A of the Ordinance.

39 "Information location tools" include directories, indexes, references, pointers, or hypertext links that refer users to an online location. See section 65A(2) of the Ordinance.

40 Paragraphs 4.15 to 4.25 of the Code.

	Notice and Takedown System (Storage)	Notice and Takedown System (Information Location Tools)	Notice and Notice System
Applicability	OSPs which have stored material or activity on their platforms at the direction of users.[41]	OSPs which have linked or referred users to an online location containing allegedly infringing material or activity, by information location tools on their platforms.[42]	OSPs which transmit, route, or provide connections for digital online communications, and which do not: • initiate the transmission; • select the recipient of the transmission except as an automatic response to the sender's request; or • select or modify the information or material being transmitted.[43]
Subject matter of the Notice	Allegedly infringing material or activity located on the platform.[44]	A link or reference on the platform which refers to allegedly infringing material or activity.[45]	An account on the platform which has been used in allegedly infringing activities.[46]
Steps to be taken by the OSP upon receiving a Notice	1. Acknowledge receipt. 2. Notify the complainant as soon as practicable if the Notice does not comply with the specified form and delivery method. 3. Otherwise, remove or disable access to the material or activity as soon as practicable. 4. Promptly notify the user in writing of the removal or disabling of access and other information specified in the Code.[47]	1. Acknowledge receipt. 2. Notify the complainant as soon as practicable if the Notice does not comply with the specified form and delivery method. 3. Otherwise, disable access to the material or activity as soon as practicable. 4. If the material or activity has been made and stored by the OSP on the platform, also remove or disable access to them as soon as practicable.[48]	1. Acknowledge receipt. 2. Notify the complainant as soon as practicable if there are grounds for not processing the Notice (e.g. if it does not comply with the specified form and delivery method, or if the account complained of is no longer valid). 3. Otherwise, notify the user in writing of the complaint and other information specified in the Code as soon as practicable.[49]

41 Paragraph 4.1 of the Code.
42 Paragraph 5.1 of the Code.
43 Paragraphs 3.1 and 3.2 of the Code.
44 Paragraph 4.3 of the Code.
45 Paragraph 5.3 of the Code.
46 Paragraph 3.4 of the Code.
47 Paragraphs 4.9 to 4.14 of the Code.
48 Paragraphs 5.8 to 5.11 of the Code.
49 Paragraphs 3.8 to 3.14 of the Code.

	Notice and Takedown System (Storage)	Notice and Takedown System (Information Location Tools)	Notice and Notice System
Counter Notice	5. The user may send a Counter Notice to the OSP within 20 working days after receiving the OSP's notice. 6. The OSP shall acknowledge receipt and promptly notify the complainant in writing of the Counter Notice. 7. The complainant has 20 working days after receiving the OSP's notice to inform the OSP in writing that it has commenced Court proceedings in Hong Kong against the infringement.50 8. If the OSP does not receive such notice in time, it shall take reasonable steps to reinstate or permit access to the material or activity.[51]	Not applicable. This system is not designed for the user to issue a Counter Notice.	Not applicable. This system is not designed for the user to issue a Counter Notice.

The Notice and Counter Notice must include certain statements and information to support or dispute the complaint, which are set out in the forms annexed to the Code ("**Standard Forms**"). An OSP may request additional information in its forms; however, it should make clear that failure to provide the additional information will not render the Notice or Counter Notice defective.[52]

Finally, the Code requires that all OSPs shall keep a record of the Notices and Counter Notices received, and any notices sent to users, for 18 months.[53]

Takeaways and Observations

- To avail themselves of the safe harbour, OSPs should ensure that their content review team is familiar with the Code. This includes being able to determine which of the three systems in the Code applies to a particular Notice, consider whether there are grounds for not processing the Notice, and handle a Counter Notice and reinstatement of the allegedly infringing material within the specified timeframe.

50 This includes applying for a court order requiring the OSP to disclose the identity of the responsible user (Paragraph 4.24(b) of the Code).

51 Paragraphs 4.15 to 4.25 of the Code.

52 Paragraphs 3.5, 4.4, 4.16, 5.4 of the Code.

53 Paragraphs 3.15, 4.26, and 5.12 of the Code.

- OSPs which do not have a take-down mechanism can make use of the practice and procedure laid out in the Code. Other OSPs should compare the Standard Forms with their corresponding set of forms, and ensure that their forms include the mandatory statements and information required by the Code. Alternatively, OSPs which operate global platforms can additionally adopt the Standard Forms for complaints that concern infringing acts conducted in Hong Kong or targeting the Hong Kong market.
- OSPs should review their compliance with the Personal Data (Privacy) Ordinance (Cap. 486) regarding the collection and processing of personal data provided in the Notices and Counter Notices. This includes taking reasonable steps to notify complainants and users respectively, of the OSPs' Personal Information Collection Statement ("**PICS**").[54] OSPs should also ensure that their platforms' Terms of Use allow them to take the appropriate notice and/or takedown actions under the Code.[55]
- The Code is silent on the timeframe in which OSPs under the "notice and takedown" system must remove or disable access to the allegedly infringing material or activity. Instead, they are asked to do so "as soon as practicable" upon receiving a valid Notice. Such flexibility is in line with the "notice and takedown" systems in other jurisdictions, such as the United States and the European Union.[56] Until there is case law on this point in the context of copyright infringement, one may look to *Oriental Press v Fevaworks*, a landmark case concerning the liability of internet intermediaries for defamatory content on their platforms.[57] In that case, the Hong Kong Courts held that the provider of an online discussion forum was not liable for defamatory statements which were removed around 3.5 hours after being notified by the claimant. However, the provider was held liable for other statements which were removed more than 8 months after being notified by the claimant.

Conclusion

The safe harbour mechanism in the Ordinance and clear guidance in the Code will no doubt be embraced by copyright owners. Despite the accessibility of filing complaints with OSPs, copyright owners should bear in mind the risk of civil and criminal liability for knowingly or recklessly filing unmeritorious complaints. A Notice which does not include sufficient particulars of the copyright work or convincing arguments on how the content is infringing, may lead to the user filing a Counter Notice, in which case the content will be reinstated unless the complainant further pursues the matter in the Hong Kong Courts. Copyright owners are therefore advised to carefully consider the merits of their claims and whether any exemptions to the potential infringement may apply. Owners should also ensure that the Notice is drafted comprehensively and evidence of the infringement is preserved before filing the Notice and alerting the relevant user.

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

54 Paragraph 1.7 of the Code.

55 Paragraph 1.6 of the Code.

56 See Section 512 to Title 17 of the United States Code and Article 14 of the Electronic Commerce Directive 2000, both requiring that service providers act expeditiously to remove, or disable access to, the allegedly infringing material.

57 Oriental Press Group Ltd and Another v. Fevaworks Solutions Ltd (04/07/2013, FACV15/2012) (2013) 16 HKCFAR 366; Oriental Press Group Ltd and Another v. Fevaworks Solutions Ltd (25/02/2011, HCA2140/2008).

Scanning the News – The Need for Fair and Equal Treatment in Election News

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

Grace Wong, Associate
Mayer Brown, Hong Kong

On 27 February 2023, the Communications Authority ("**CA**") issued a press release summarising its decision against HK Television Entertainment Company Limited ("**HKTVE**") with respect to its news coverage on candidates running for the 2021 Legislative Counsel General Election ("**Election**") on its ViuTV Channel ("**Programme**").[58]

Relevant Code of Practice and Guidelines

Television programme service licensees, including domestic free television programme service providers such as the HKTVE,[59] are required to comply with the Broadcasting Ordinance (Cap. 562), the Broadcasting (Miscellaneous Provisions) Ordinance (Cap. 391), and related subsidiary legislation. These provisions are supplemented by the terms and conditions of the relevant licenses, as well as mandatory Codes of Practice issued by the CA.

58 Original text of the press release can be found at Communications Authority - Press Releases (Record No.: 2311) (coms-auth.hk).

59 The four categories of licensed television programme services are (i) domestic free television programme services, (ii) domestic pay television programme services, (iii) non-domestic television programme services and (iv) other licensable television programme services.

These include the Generic Code of Practice on Television Programme Standards ("**Code**"), which sets out general programme standards and other principles on scheduling, use of language, and indirect advertising etc.[60] Among other principles, all licensees are required to preserve due impartiality in news programmes and to present opposing points of view in a balanced manner.[61] Domestic free and domestic pay television programme services shall also observe all elections-related regulations and guidelines issued by the Electoral Affairs Commission ("**EAC**").[62]

In its present decision, the CA found that HKTVE did not fully observe the EAC's Guidelines on Election-related Activities in respect of the Legislative Council Election ("**Guidelines**"). Under the Guidelines, media organizations should ensure that fair and equal treatment is given to all candidates when covering elections. Favourable or unfavourable treatment should not be given to any candidate, and media organizations should make sure that their programmes or reports do not constitute election advertisements.[63]

Accordingly, the names of all candidates of the same constituency should be mentioned in a news report:

"Election-related news involving a particular candidate can be reported by itself even if no other news on other candidates is carried that day. However, the other candidates of the same constituency must at least be mentioned. The mention should be made in the same programme or publication by the media in an appropriate way. They may not necessarily appear within the content of the same report, but in principle, should enable the viewers, listeners or readers to be informed of the other candidates."[64]

Handling of Broadcast Complaints

Complaints about potential contraventions of television broadcasting legislations, license conditions or Codes of Practice, are made to the CA in accordance with the procedure in the Broadcasting (Miscellaneous Provisions) Ordinance. A complaint which contains *prima facie* evidence of a breach will be referred to the Broadcast Complaints Committee ("**BCC**"). The BCC will make recommendations to the CA after reviewing the material under complaint and considering the licensee's representations. The CA will then invite the licensee to make further representations and make its final decision.[65]

If a contravention is found, the CA may advise the licensee to pay closer attention to the relevant provisions or issue a warning against future violation.[66] In serious cases, the CA may impose a penalty, direct the licensee to include a correction and/or apology in its television programme services, or even suspend or recommend that the license be revoked.[67]

If the licensee wishes to contest the CA's decision, it may either appeal by way of petition to the Chief Executive in Council, or by way of judicial review to the Court of First Instance.[68]

The Decision

The cause for complaint against the Programme was that it only mentioned some of the candidates running in different geographical or functional constituencies in the Election. Instead of mentioning the names of all candidates in those constituencies or showing their names on the screen, the Programme showed two QR codes at the end of the news report that linked to the information of all candidates and the news anchor urged viewers to scan the codes.

60 Original text of the Code can be found at code_tvprog_e.pdf (coms-auth.hk).

61 Paragraphs 2 to 5, Chapter 9 of the Code.

62 Paragraph 9, Chapter 12 of the Code.

63 Part I, Chapter 12 of the Guidelines which can be found at Chapter 12 (eac.hk).

64 Paragraph 12.8, Chapter 12 of the Guidelines.

65 The Broadcast Complaint Handling Procedures of the Communications Authority.

66 Section 24 of the Broadcasting Ordinance.

67 Sections 28 to 33 of the Broadcasting Ordinance.

68 Section 34 of the Broadcasting Ordinance; Television Broadcasts Ltd v. Communications Authority and Another (29/01/2016, HCAL176/2013) [2016] 2 HKLRD 41, para. 142.

The CA agreed with the EAC that HKTVE failed to mention the names of all candidates of the same constituency in the Programme, as required by the Guidelines. HKTVE was therefore in breach of the Code. As HKTVE had examined its internal process to ensure that it will comply with the relevant requirement, the CA advised HKTVE to observe the relevant provision in the Code more closely and did not impose any sanction.

Takeaway

This decision goes to show that the CA does not deem the use of QR codes as a mechanism to satisfy the requirement of showing the information "in the same programme or publication". Whilst the CA did not elaborate on its decision in its press release, it may have taken into account the fact that not all viewers would watch the end of the news report; and even if they did, they may not be technology-savvy enough to scan the QR codes.

Contact Us

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

Amita Haylock
Partner
+65 6922 2311
+852 2843 2579
amita.haylock
@mayerbrown.com

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

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

Grace Y. Wong
Associate
+852 2843 2378
grace.wong
@mayerbrown.com