Third Quarter 2015

MAYER·BROWN JSM

IP & TMT Quarterly Review

Table of Contents

Copyright – China

China's Cloud Gate and Copyright Protection

By Rosita Li, Partner, Mayer Brown JSM, Hong Kong
Maggie Lee, Legal Assistant, Mayer Brown JSM, Hong Kong

A sculpture in Karamy, Xinjiang, China has recently caught much media attention because of its striking similarities with the famous bean-shaped sculpture in Chicago, "Cloud Gate".

Cloud Gate has been a landmark of the Chicago landscape since it was installed outside the Art Institute of Chicago and Millennium Park in 2006. With a polished silvery exterior, Cloud Gate is famous for its reflection of Chicago's skyline. A unique structure, Cloud Gate has an arc underneath large enough for visitors to walk through. In "contrast", the sculpture in China is supposed to mimic an oil bubble and is a reference to an oil well in Karamy. The Chinese installation also has a mirror-like surface and passages that lead to the under-belly of the "oil bubble".

When Anish Kapoor, the author of Cloud Gate, learned about the sculpture in China, he said: "It seems that in China today it is permissible to steal the creativity of others, I feel I must take this to the highest level and pursue those responsible in the courts."[1]

How is copyright in a sculpture like Cloud Gate protected internationally? How can an author pursue a claim in China?

INTERNATIONAL COPYRIGHT PROTECTION – HOW DOES IT WORK?

The first thing to note is that there is no right known as "international copyright", meaning there is no uniform set of laws that governs copyright in a work around the world. Copyright law is "territorial" in nature, meaning that the copyright protection afforded to a work in a certain jurisdiction depends on the national laws of the jurisdiction in which the author seeks protection, and the various copyright international conventions to which the respective country may or may not be signatory.

In Hong Kong, copyright subsists in certain types of works, including artistic works such as sculptures and paintings. It is not necessary to register copyright in Hong Kong in order to obtain protection under the Copyright Ordinance (Cap. 582). As an artistic work, copyright automatically subsists in a sculpture at the time of creation.

Through the application of international copyright conventions, a sculpture created in Hong Kong also enjoys protection in most countries around the world. The most significant international treaty that governs international protection of copyright is The Berne Convention for Protection of Literary and Artistic Works ("**the Berne Convention**"). Some of its key features are:

- National treatment – Works originating in one contracting state must be given the same protection in each other contracting state as the latter grants protection to the works of its own nationals; and
- "Automatic" protection – No formalities are required to be complied with in the other contracting states.

1 http://blogs.wsj.com/chinarealtime/2015/08/12/a-cloud-gate-in-china-xinjiang-sculpture-resembles-chicago-bean/

At present, there are 168 contracting states to the Berne Convention. As China (extending to Hong Kong) is a signatory to the Berne Convention, copyright works created in Hong Kong and in all other contracting states of the Berne Convention are also automatically protected in China, according to China's copyright law.

CHINA'S COPYRIGHT LAW

Under China's copyright law, copyright subsists in works of fine art and architecture, including a sculpture.[2] Any person who copies another's work commits an act of copyright infringement and should bear civil liability.[3] Any person who reproduces a work without the author's permission (the "**Infringing Act**") is also civilly liable.[4] Furthermore, if the Infringing Act is considered to harm the public interest, the state and local copyright administration departments have the power to order the infringer to cease the Infringing Act, confiscate his illegal gains, confiscate and destroy the reproductions of the work, and impose a fine on the infringer. [5]

Should an author wish to pursue a copyright claim in China, he would need to collect evidence of infringement and will have a choice of pursing his claim by way of an administrative action or a civil action.

CHALLENGES IN ENFORCEMENT IN CHINA

Foreign authors often face difficulties when enforcing copyright works in China for the following reasons:

1. Differences between China's copyright law and foreign copyright law and lack of understanding of the Berne Convention

   China maintains a system of voluntary copyright registration[6] and domestic enforcement actions are often based on registered copyright rights. If the copyright in question has not been registered in China, enforcement agencies may be reluctant to assist with copyright infringement investigations as they may not understand the effects of the Berne Convention.

2. Local protectionism

   Enforcement agencies in China may be protective of local companies and individuals. They may also be reluctant to take action due to feared impact on the local economy.

3. Political institutions in China might have vested interests in certain industry sectors and their interests may collide with the interests of foreign investors and their copyright and other intellectual property rights

   Enforcement agencies may often face political pressure and incline to favour political institutions in enforcement actions.

2 Article 3 of the Copyright Law of the People's Republic of China and Article 4 of the Regulation for the Implementation of the Copyright Law of the People's Republic of China

3 Article 47 of the Copyright Law of the People's Republic of China

4 Article 48 of the Copyright Law of the People's Republic of China

5 Article 48 of the Copyright Law of the People's Republic of China

6 See Temporary Measures on the Voluntary Copyright Registration of Works issued by National Copyright Administration of China

4. Limited manpower and resources dedicated to enforcement in China, especially in smaller and lower tier cities.

As a result of these challenges, many foreign authors and innovators have been put off from enforcing their rights in China.

FINAL REMARKS

In recent years, the Chinese government has made tremendous efforts to address intellectual property rights problems and improve enforcement efficiency, such as by updating its laws and establishing specialised IP courts. It is hoped that China will continue to increase the transparency and certainty of enforcement actions, so that intellectual property right owners will not hesitate to enforce their rights and China will become a more innovation-friendly country for both authors and innovators domestically and internationally. Meanwhile, please watch this space to see if Kapoor will really take the "China's Cloud Gate" case to the courts in China.

Trade Marks – Hong Kong

Your Mooncake or Mine: An Exploration of the Defence of Honest Concurrent Use in Trademark Invalidation

By Benjamin Choi, Partner, Mayer Brown JSM, Hong Kong
Nicola Kung, Associate, Mayer Brown JSM, Hong Kong

Lin Heung Tea House & Bakery v Guangzhou Catering Services Enterprises Group Co Ltd [2015] 4 HKC 333 is a recent Court of Appeal ("**CA**") case involving a trademark dispute between two mooncake companies. Both companies sold mooncakes under the mark "莲香" (translation: lotus fragrance). The CA upheld the decision of the Court of First Instance ("**CFI**") to invalidate Guangzhou Catering Services Enterprises Group Co Ltd's (the "**Appellant's**") registered trademark "莲香" (the "**Suit Mark**") based on the other side's unregistered marks. Although both the CA and CFI concluded that the Suit Mark should be invalidated, the Appellant's defence of honest concurrent use was treated and analysed quite differently by the two Courts.

BACKGROUND

When a party applies to register a trademark at the TM registry, the Registrar will assess the application and decide whether the mark meets the requirements for registration. There are two grounds on which a trademark application may be refused:

- **Absolute grounds**: the mark will be assessed on its own to see whether it contravenes any of the basic requirements of a trademark. For example, the mark cannot be registered if it is devoid of distinctive character, or if the mark is solely descriptive of any characteristics of the goods or services for which it will be used. These are known as absolute grounds of refusal.
- **Relative grounds**: the mark will be assessed in relation to existing marks. If the applied-for mark is too similar to a trademark that has already been registered, or if it is too similar to an earlier mark which is protected by the law of passing off, then it will also be rejected. These are known as relative grounds of refusal.

Likewise, an existing trademark registration can be challenged on both absolute grounds and relative grounds. If the challenge is successful, then the trademark will be invalidated.

In both trademark applications and invalidations, a relative ground of refusal can be overcome by proof of honest concurrent use.

FACTS

In 2006, Lin Heung Tea House & Bakery (莲香茶楼及饼家) ("**LH Bakery**") applied to register the marks "莲香" and "莲香楼" in Hong Kong. However LH Bakery's applications were rejected by the Registrar of Trade Marks because the Suit Mark, also consisting of the characters "莲香", had already been registered in Hong Kong in 1996. The Suit Mark was originally registered by Guangzhou Lianxiang Lou ("**GLX**"). GLX assigned the Suit Mark to the Appellant in 2006. The two companies used the same name "莲香" because they shared a common origin. Both LH Bakery and the Appellant can be traced back to GLX, which was founded in 1910. For historical reasons, the two companies used almost identical mooncake packaging designs.

COURT OF FIRST INSTANCE DECISION (HCMP 133/2008)

In an effort to stop the Suit Mark citation from blocking its trademark applications, LH Bakery commenced a Court action to have the Suit Mark invalidated. LH Bakery succeeded in its invalidation action based on two relative grounds :

1. **Passing off**: at the time the Suit Mark was registered, LH Bakery had earlier unregistered trademarks, "莲香" and "莲香楼", and could seek protection based on the common law tort of passing off. LH Bakery was therefore entitled to prevent the use and registration of the Suit Mark.
2. **Well-known mark**: the Suit Mark is identical to LH Bakery's earlier trademark which, at the time of registration, was already protected as a well-known mark. The use of the Suit Mark would take unfair advantage, or be detrimental to the distinctive character or repute of the earlier mark.

The Appellant attempted to rely on the defence of honest concurrent use in this invalidation action. As the Appellant did not acquire the Suit Mark until 2006, the arguments put forward were centred on the use of the Suit Mark by the assignor of the mark, GLX. The Appellant's argument was that their mooncakes had been sold by GLX in boxes bearing the trade name "广州莲香楼" and the tagline "莲香饼好月团圆" since 1984. Therefore, when the Suit Mark was registered in 1996, even if LH Bakery's marks could be protected by the common law of passing off or as well-known marks, a case of honest concurrent use of the Suit Mark could be made out. Therefore the Suit Mark should not be invalidated.

The CFI rejected this argument, considering that GLX's actual use of the Suit Mark was always in conjunction with "广州" or in the form of "广州莲香楼". As this was "*not a use of the suit mark simpliciter*" (i.e., not just 莲香 by itself), there was no honest concurrent use of the Suit Mark on its own.

The CFI judge gave judgment for LH Bakery, declaring the Suit Mark invalid.

COURT OF APPEAL DECISION

The Appellant's appeal of the CFI decision was focused solely on the CFI's rejection of their defence of honest concurrent use.

The CA applied the two-stage test for determining whether there has been honest concurrent use, as stated in *Re CSS Jewellery Co Ltd* [2010] 1 HKC 563:

- Stage 1 - whether there has been an honest concurrent use of the subject mark (i.e., the Suit Mark) and the earlier trademark (i.e., LH Bakery's marks).
- Stage 2 - if the answer is yes, whether after considering all the relevant circumstances, including public interest, the Registrar should exercise its discretion to accept the registration of the subject mark (i.e., the Suit Mark) despite that the use of the mark is likely to cause public confusion.

Stage 1 – Honest concurrent use

a. *Use as a trademark simpliciter*

The Appellant argued that the CFI should have held that there had been use of the Suit Mark *simpliciter* and as a trade mark by GLX. Various examples of the use of the Suit Mark on GLX's mooncake packaging were cited: "莲香月饼" (Lianxiang

Mooncake) "广州莲香老饼家" (Guangzhou Lianxiang Old Bakery) and "广州莲香楼" (Guangzhou Lianxiang House). The Appellant argued that in all these examples, "莲香" was the only distinctive term. All the other words – "月饼" (mooncake), "月饼" (Guangzhou), "老饼家" (old bakery) and "楼" (house) were purely descriptive. Therefore, there had been use of the Suit Mark simpliciter by GLX.

The CA accepted this argument and considered that the CFI was wrong to hold that GLX's use of the Suit Mark was not honest concurrent use because it was not use of the mark as a trade mark *simpliciter*. The CA clarified that the term "trade mark *simpliciter*" is not a legal term. All that it means is that the trade mark is not used on its own, but in connection with other marks or descriptive elements. Just because a trade mark is not used on its own does not mean that it is not being used as a trade mark.

b. *Honesty*

LH Bakery challenged the honesty of GLX's use of the Suit Mark and argued that the Stage 1 inquiry focuses on three matters (i) use; (ii) concurrent use; and (iii) honesty of the concurrent use. When considering the question of honesty in part (iii), the Court should take into account the knowledge of the party seeking to rely on the defence of honest concurrent use. The CA accepted that this was a well founded submission.

LH Bakery argued that GLX had used the Suit Mark in conjunction with "广州" (Guangzhou) or in the form of "广州莲香楼" (Guangzhou Lianxiang House) to avoid confusion and to distinguish their mooncakes from those of LH Bakery. Accordingly, GLX's (i) knowledge of the likelihood of confusion; and (ii) their attempt to avoid confusion by using the Suit Mark in conjunction with other indicia was relevant to the question of honesty.

The CA rejected this argument, stating that "*it has to be stressed that not every knowledge of the existence of an earlier mark or the likelihood of confusion with such an earlier mark or the need to use some safeguards to avoid confusion will render the use dishonest". Further, "even if the mark is being used in combination with other words, the purpose of which is to prevent confusion, this cannot be regarded as evidence of dishonesty.*"

The CA found that GLX had indeed satisfied the Stage 1 requirement of honest concurrent use.

Stage 2 – Registrar's discretion

Stage 2 required a balancing exercise as to whether discretion should be exercised to allow the registration despite the fact that it would cause a likelihood of confusion. In carrying out this balancing exercise, the CA gave particular weight to the following:

- **Period of use:** the Suit Mark had only been used by GLX in Hong Kong between 1984 and 2006 (22 years), whereas LH Bakery has been carrying on its restaurant and mooncake business in Hong Kong under the trade mark "莲香" for over 80 years. "莲香" has since become a well-known local brand, associated with LH Bakery's restaurant and mooncakes.

- **Lack of use:** by the time of the CFI trial, 5 years had elapsed since the last use of the Suit Mark in Hong Kong. Even before that, the sale of GLX's mooncakes in Hong Kong had dwindled to a very low figure, with an annual turnover of less than HK$100,000. In comparison, LH Bakery was still selling 莲香 mooncakes in Hong Kong, and reporting impressive annual sales of HK$3.6 million.
- **Prejudice:** due to the lack of use of the Suit Mark, the CA decided that if discretion was exercised against the Appellant, it would suffer relatively little inconvenience. No serious prejudice would be caused to it if it were required to change its packaging as a result of the Suit Mark being declared invalid.

The CA therefore decided that discretion should not be exercised to let the Suit Mark remain registered as the Appellant could not satisfy Stage 2 of the two-stage test. As a result, the CFI's decision to invalidate the Suit Mark based on the relative grounds of refusal was upheld by the CA.

CONCLUSION

This case illustrates to what extent and under what circumstances the defence of honest concurrent use may work, clarifying two important points in the application of the *Re CSS Jewellery Co Ltd* two-stage test. First, just because a trade mark is not being used on its own (but in combination with other solely descriptive elements) does not mean that it cannot satisfy the usual trade mark use requirement. Secondly, when carrying out the balancing exercise in Stage 2 of the *Re CSS Jewellery Co Ltd* test, the Court will pay particular attention to the extent of actual use of the mark in question and other relevant circumstances. In this case, LH Bakery succeeded in invalidating an existing registration of an identical mark to clear the way for registering their long used but unregistered "莲香" and "莲香楼" trade marks. The Court's discretion might not have been exercised the same way if the Appellant had been selling its moon-cakes in Hong Kong continuously and extensively getting a decent revenue, or if LH Bakery's business was not as famous. This case has alerted trademark owners of the importance of making actual, genuine use of their registered trademarks. Despite the fame of LH Bakery and its abundant use of the"莲香" and "莲香楼" trade marks, it still took LH Bakery nine years to resolve this case with its competitor who had been operating in Hong Kong for a considerable period of time.

Child's Play: Protecting the Privacy of Minors Online

By Gabriela Kennedy, Partner, Mayer Brown JSM, Hong Kong
Karen H.L. Lee, Associate, Mayer Brown JSM, Hong Kong

What parent has not dealt with a huffy teenager demanding that parents "respect their privacy" and "keep out" of their room? Whilst children may be concerned about maintaining their privacy vis-a-vis their parents, their own increasing use of social media and voluntary disclosure of private information seems to send a conflicting message. The large number of photos, status updates, posts, etc, by the younger generation, seems to suggest a cavalier attitude to privacy and little or no concern about the potential implications of making such personal data publicly available. Has a teenager really thought carefully before he posted that photo of himself misbehaving during a night out drinking with friends? Has he really considered the future implications of a photo being spotted by a future employer or university admissions officer?

In May 2015, the former Hong Kong Privacy Commissioner ("**PC**") announced the results of a study carried out in October 2014, which revealed that children are now going online at a much younger age than ever before. The study also revealed a fundamental lack of awareness of the serious risks that are posed to a child's data privacy in their online activities by children, parents and teachers alike.

PERSONAL DATA ONLINE

Following an incident in May 2015, when a Hong Kong pro-government group was accused of posting a video online showing students supporting the proposed electoral reform package, without the students' consent, the former PC turned his attention to the issue of the online protection of young people's personal data. The video was made as part of an application for a study tour to the USA. The students alleged that the pro-government group had assured them that the video would not be made public.

Complaints with regard to this incident were made to the former PC, and a formal investigation may be launched at a later date. In the meantime, the former PC issued a media statement on 13 May 2015, reminding organisations of the need to comply with the Hong Kong Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**") in the collection and use of personal data, including personal data of minors[7]. This includes taking all practicable steps, on or before the collection of the personal data, to notify the relevant data subjects (i.e., the children) of the purpose for which their data is being collected and the classes of persons to whom their data may be transferred[8], and not using the data for any other purpose, than the purpose for which it was collected, unless with the express prior consent of the data subject[9].

On 11 May 2015, the former PC also announced that he had joined the Global Privacy Enforcement Network (along with 27 other data privacy enforcement authorities) to conduct a Privacy Sweep that would examine websites and mobile apps to determine whether or not there

7 https://www.pcpd.org.hk/english/news_events/media_statements/press_20150513.html

8 Data Protection Principle 1 of the PDPO.

9 Data Protection Principle 3 of the PDPO.

are any issues regarding the personal data of minors[10]. The Privacy Sweep took place between 11 to 15 May 2015, and the results will be announced later this year.

In addition to being the class of most active users of the Internet, mobile apps and social networks, the young generation is also seen as one of the most vulnerable groups of data subjects. It is very likely that the results of the Privacy Sweep will be combined with the issuance of guidelines on how to educate the public on the steps that need to be taken to protect the privacy of minors.

RESPONSIBILITY OF SCHOOLS AND OTHER ORGANISATIONS

Schools and other organisations need to be cautious when collecting and using the personal data of children. Their obligations under the PDPO apply equally to minors as they do to adults. Schools, in particular, should ensure they have in place internal guidelines and codes of practice consistent with the provision of the law on the collection, use and retention of their students' personal data (including any former students or student applicants) and their families.

When collecting personal data of youngsters, it is important to ensure (amongst other things) that:

a. The personal data collected is not excessive, and is needed for a purpose directly related to the data user's functions or activities;
b. The data subject must have been informed on or before personal data was collected, of the purpose for which their data will be used and to whom it may be transferred – the wording used in the notification should be tailored towards the age group of the data subjects, and should use simple language that is easy to understand;
c. The personal data is not kept longer than is necessary in order for the purpose in which it was collected; and
d. The personal data is securely stored and safeguarded from unauthorised access, loss or damage.

An area to which schools and other organisations should also pay particular attention, is their obligation to comply with data access requests under the PDPO. Under the PDPO, a data access request may be made on behalf of a minor by their parent or guardian[11]. However, steps must be taken to ensure that the person making the request is authorised to do so on behalf of the minor, e.g., evidence should be provided showing that the requestor is the parent of the minor. Even if it is established that the requestor is a "relevant person", i.e., a parent or guardian, this does not necessarily mean that the school or other organisation should automatically comply with the data access request. It should only comply with the request, if it is satisfied that such is made "on behalf of" the minor, and not for the parent or guardian's own purposes. The nature of the data being requested may in itself make it sufficiently clear that the request is not being made for the benefit of the minor. For example, if a parent issues a data access request to a school asking for the address of his/her child, this should raise alarm bells with the school, since the child would clearly already know his own address, and would not need to issue a data access request to the school to obtain it. Therefore, the logical conclusion would be that the parent is likely making the data access request to further his/her own interest (e.g., to discover

10 https://www.pcpd.org.hk/english/news_events/media_statements/press_20150511.html

11 Section 18(1) of the PDPO.

the location of the child who he may be denied access to by the court). In such circumstances, it is better for the school to exercise caution and seek evidence and/or an explanation from the parent as to why they are making the data access request, and possibly talk to the other parent or guardian of the minor.

CONCLUSION

Particular caution needs to be taken when collecting personal data from minors, due to the vulnerable nature of the group. It is likely that the new PC (who took office on 4 August 2015) will decide to issue guidance notes or take enforcement action against data users, especially those that target youngsters (e.g., online gaming companies), following the announcement of the results of its Privacy Sweep later this year. Proactive steps should be taken by schools and other organisations to conduct an internal data privacy audit (including a review of their personal information collection statements, their data retention policies, etc), to ensure compliance with the PDPO.

The End of an Era: Outgoing Hong Kong Privacy Commissioner in Flurry of Activity in Last Months in Office

By Gabriela Kennedy, Partner, Mayer Brown JSM, Hong Kong
Karen H.L. Lee, Associate, Mayer Brown JSM, Hong Kong

On 4 August 2015, Mr. Stephen Kai-Yi Wong took office as the new Privacy Commissioner of Hong Kong. Mr. Wong replaced Mr. Allan Yan-Wang Chiang, following the completion of his five year term.

LEAVING WITH A BANG

Former Privacy Commissioner, Allan Chiang, kept himself very busy in the months leading up to the end of his term in the office. In July 2015 alone, his office issued: (i) an Information Leaflet on minimising data privacy risks when using smartphones; (ii) an Information Leaflet on cloud computing; (iii) a Guidance Note on the collection and use of biometric data; and (iv) a media statement urging the government to tighten controls over the protection of personal data on public registers in the current era of big data.

Mr. Chiang's tenure as the Privacy Commissioner will be remembered for:

- The launch of the Privacy Management Programme on 18 February 2014, an initiative that encourages organisations to proactively embrace personal data protection as part of their general corporate governance responsibilities, rather than merely as a legal compliance issue[12];
- Active participation in the Asia-Pacific Economic Cooperation ("**APEC**") activities, including assisting in the drafting of the Cross Border Privacy Rules in 2011, as part of the APEC Data Privacy Framework, which promotes a consistent approach to data privacy protection in the Asia Pacific region.
- Issuance of 17 Guidance Notes, 8 Information Leaflets, 1 Code of Practice and 2 explanatory documents, many of which relate to technological advancements and their impact on data privacy (e.g., mobile apps, biometric data, drones, cloud computing, use of public data) and the provision of specific guidance to certain industries (e.g., the banking and finance industry, information technology service providers, the insurance industry, etc);
- Active enforcement of the legislation, with 31 Investigation Reports out of the 44 Investigation Reports ever issued since the Personal Data (Privacy) Ordinance ("**PDPO**") was enacted, being issued during Mr. Chiang's 5 year tenure, with the actual number of enforcement notices peaking at 90 for the year 2014. The apex of enforcement actions was the Investigation Report that was triggered by the Octopus cards débacle, which led to amendments to the PDPO, and the referral of cases for prosecution, notably the one resulting in the first imprisonment ever for a breach of the PDPO, as a result of a false statement made during an investigation (an offence under Section 50B(1)(b)(i) of the PDPO)[13].

12 See our article entitled Moving from Compliance to Accountability – the Privacy Commissioner of Hong Kong Issues Best Practice Guide on Privacy Management Programme: http://www.mayerbrown.com/files/Publication/e8e17e07-4f6d-4862-a8a6-ba15cc7b2d4c/Presentation/PublicationAttachment/c6d1f518-adbe-407e-b3cd-de70f34d367c/IP_TMT_QuarterlyReview_2014Q1.pdf

13 See our article entitled First Person to be Imprisoned under the Hong Kong Personal Data (Privacy) Ordinance: https://www.

A NEW ERA?

Since the changing of the guards on 4 August 2015, the Office of the Privacy Commissioner has issued the Guidance Note on Electioneering Activities (no doubt a nod in the direction of the upcoming District Council elections), and has issued statements in connection with the much publicised first conviction for a breach of the direct marketing provisions. In media interviews, the new Privacy Commissioner has stressed the need to balance the protection of individuals' rights with safeguarding the role of Hong Kong in the global marketplace by maintaining a free flow of information. A significant emphasis will be placed on educating businesses, with the aim of moving the needle from compliance to accountability. These are well-known tunes, but the magic, as in music, will lie in their "arrangement" and the skills and technique of the "new conductor" leading our top-class orchestra for the next five years.

mayerbrown.com/First-Person-to-be-Imprisoned-under-the-Hong-Kong-Personal-Data-Privacy-Ordinance-01-20-2015/

Two Companies Convicted for Breach of the Direct Marketing Provisions under the Hong Kong Personal Data (Privacy) Ordinance

By Gabriela Kennedy, Partner, Mayer Brown JSM, Hong Kong
Karen H.L. Lee, Associate, Mayer Brown JSM, Hong Kong

On 9 and 14 September 2015, Hong Kong Broadband Network Limited and Links International Relocation Limited respectively were convicted for breaching the direct marketing provisions under the Personal Data (Privacy) Ordinance ("**PDPO**"). These are the first set of convictions issued under the direct marketing provisions in Hong Kong which came into effect on 1 April 2013.

THE DIRECT MARKETING PROVISIONS

On 27 June 2012, the Personal Data (Privacy) (Amendment) Ordinance 2012 ("**Amendment Ordinance 2012**") was passed. Some of the amendments came into force on 1 October 2012, whilst the direct marketing and legal assistance provisions came into force on 1 April 2013.

In brief, the effect of the restrictions on direct marketing is that data users cannot use an individual's personal data in direct marketing, or transfer such personal data to a third party for their use in direct marketing, without that individual's express prior consent[14]. In order to obtain valid consent, the data user must notify the individual of the following pursuant to Section 35C of the PDPO:

a. That it intends to use their personal data for direct marketing, and cannot do so without their consent;
b. The type of personal data that will be used;
c. The classes of goods, facilities or services that will be advertised; and
d. (A response channel through which the individual can communicate his/her consent (without charge).

If a data user also intends to transfer the personal data to a third party for their use in direct marketing, then, in addition to the above notice, the data user must notify the individuals of the classes of transferees to whom their personal data may be transferred, and whether the personal data will be transferred for gain[15].

Silence or a lack of response from an individual will not amount to valid consent for the purposes of direct marketing. In addition, when an individual's personal data is used for the first time in direct marketing, i.e., when the first marketing email is sent, then the data user must notify the individual that they can opt-out of receiving such direct marketing communications at any time, and must provide them with a means to communicate such withdrawal of consent[16].

A notice from a data subject requesting the cessation of use of their personal data for direct marketing purposes must be complied with promptly[17] irrespective of the timing of such request (i.e., whether it comes after the first instance of direct marketing or later).

14 Section 35E and 35K of the PDPO.
15 Section 35J of the PDPO.
16 Section 35F of the PDPO.
17 Section 35G of the PDPO.

A breach of the direct marketing provisions is a criminal offence and depending on the breach may result in a maximum fine of HK$500,000 and up to 3 years imprisonment or a fine of HK$1,000,000 and up to 5 years imprisonment.

THE HONG KONG BROADBAND NETWORK LIMITED CASE

In May 2013, a month after the direct marketing provisions came into effect, the Privacy Commissioner ("**PC**") received a complaint from a customer of Hong Kong Broadband Network Limited ("**HKBN**"). Readers may remember that just before the direct marketing provisions came into force on 1st April 2013, there was a flurry of activity as many companies sent notices to customers relating to their privacy policies. We mention in passing that most of these notices were inadequate and/or counterproductive, with many data subjects being prompted by such notices to request that they be unsubscribed from marketing lists and/or to scrutinise the small print.

In this case, the complainant alleged that he had sent an opt-out request to HKBN in April 2013 by email and post. HKBN acknowledged receipt of the opt-out request in writing. However, in May 2013, the complainant received a voice message from HKBN, which notified him of the upcoming termination of his service contract, and also further promoted the services of HKBN.

After receiving the complaint in May 2013, the PC referred the matter for prosecution. HKBN was subsequently charged for failing to cease using the complainant's personal data in direct marketing after receiving the complainant's request, in breach of Section 35G(3) of the PDPO. The case was heard before the Tsuen Wan Magistrates Court. HKBN entered a plea of not guilty.

During the trial, HKBN testified that the purpose of the call was to notify the complainant that his service contract was coming to an end, and that it had provided scripts to its staff to prevent a breach of the PDPO.

Upon reviewing the evidence, the magistrate found that the true purpose of the call was to promote HKBN's services and to try and convince the complainant to renew his contract – the "reminder" that the complainant's contract was coming to an end was simply used as an opener to the direct marketing activities. The magistrate's decision was partly based on the fact that HKBN had trained its employees to continue calling the complainant even though he was unavailable, and that the call had been made more than 6 months before the complainant's service contract was set to expire. The magistrate also found that a mere written notice or text message from HKBN to the customer about the termination of the service would have sufficed, if the true intent was merely to remind the complainant such expiration.

As a result, HKBN was found to have committed an offence under Section 35G of the PDPO, and was ordered to pay a fine of HK$30,000.

HKBN has stated that it intends to appeal the decision.

THE LINKS INTERNATIONAL RELOCATION LIMITED CASE

In November 2013, the PC received a complaint from a customer of a storage company ("**Company A**"), whose business was later taken over by Links International Relocation Limited ("**Links**"). The complainant had previously hired Company A to provide storage services to him, and he had provided his personal data to Company A for such purpose (e.g., name, residential

address, company email address, mobile number and credit card details). Company A ceased operations and its business was taken over by Links. Links sent a direct marketing email to the complainant in August 2013. In the email, Links identified the complainant by name and provided the complainant with an unsolicited quotation for its storage services, as well as its standard terms and conditions. The complainant was not a customer of Links and had not been notified about his use of personal data nor had he given consent about the use of his personal data for direct marketing.

After receiving the complaint, the PC referred the matter to the police for criminal investigation. On 7 September 2015, Links was charged at the Eastern Magistrates Court for breach of Section 35C of the PDPO, namely failure to take the specified steps, including obtaining the data subject's consent, before using his data for direct marketing purposes.

Links pleaded guilty and on 14 September 2015 it was fined HK$10,000.

HARD-LINE APPROACH?

The actual fines imposed on HKBN and Links respectively are relatively small. The fine imposed on Links for example is no higher than the fines under the old and more limited direct marketing provisions before the 2013 amendments. However, unlike before when convictions under the old direct marketing provisions went unreported this time the reputational damage cannot be ignored as the convictions have made headlines. Such headlines lead to erosion of customer trust and prevention, as always, is better than cure.

We expect that more cases relating to the direct marketing provisions will come before the courts in the future resulting in more fines and even prison sentences where perhaps more egregious circumstances warrant them.

We also expect to see the Hong Kong courts imposing fines and prison sentences for breaches of Section 50A (which makes it an offence to breach an enforcement notice issued by the PC) and possibly Section 64 (which makes it an offence for a person to disclose any personal data obtained from a data user without that data user's consent in certain circumstances, e.g., a rogue employee selling personal data to a competitor).

TAKEAWAY POINTS

The recent cases highlight the fact that even notifying a customer of the data user's services, or of any deals or offers in relation to existing services, amounts to direct marketing and, unless such marketing has been sanctioned by the data subject, the notification will be carried out in breach of the PDPO. An enforcement action in such a scenario is not just a risk, but almost a certainty.

Data users are reminded to: (i) comply with notification obligations under the PDPO and obtain an individual's prior consent before using their personal data for any form of direct marketing; (ii) maintain accurate and up-to-date opt-out lists; and (iii) offer training and monitoring of front-line staff who deal with customers as scripts and template emails provided to them are no adequate substitute.

Technology – China

China's New Security Laws: Making Sense of the Fine Print

By Xiaoyan Zhang, Counsel (New York, USA), Mayer Brown JSM, Hong Kong
Maryellen Ko, Legal Assistant,, Mayer Brown JSM, Hong Kong

China sees an active landscape in security regulations in the past six months. Three major national and cyber security laws were released. Among them, the Guidelines on Promoting the Application of Secure and Controllable Information Technology in the Banking Industry ("**CBRC Guidelines**") issued by the China Banking Regulatory Commission ("**CBRC**") in late 2014 served as a kickoff.

The strong elements of data localisation displayed in the CBRC Guidelines faced complaints from foreign trade groups, including computer software giants such as Microsoft and IBM who are members of the IT Industry Council. Although China agreed to delay the implementation of the CBRC Guidelines in April 2015, not long after (1 July 2015) the National People's Congress ("**NPC**") passed the National Security Law ("**NSL**"). A week later, the NPC released the first draft of China's Cyber-Security Law ("**CSL**") for public comment. Both the NSL and the CSL contain recurring themes and broad-brushed provisions which leave much open for interpretation.

This article will examine several key provisions in these Chinese security laws, and will consider the challenges the laws pose to international companies with operations in China and propose strategies to address such challenges.

CBRC GUIDELINES ON DATA LOCALISATION

The concept of data localisation has become a popular phenomenon in recent international development, seen particularly in Russian and Chinese legislation. Whilst it can be represented in different forms, data localisation laws are at its core a type of cross-border data transfer restriction, whereby the storage, movement and processing of data is limited to specific delineated geographies. Other more direct or visible data localisation requirements include restricting the place of incorporation of any companies that manage data, the local ownership of any data storage equipment, local hiring of personnel processing data, and even down to details such as the type and make of IT equipment used.

The CBRC Guidelines was one such example of data localisation legislation, subjecting any banking financial institution "duly established within the territory of the PRC". One key recurring concept amongst the security laws is the idea that information technology must be "secure and controllable". To achieve this, the CBRC Guidelines require IT products owned or used by banks to meet a "secure and controllable" standard by, *inter alia*, registering the software source code and encryption technology with the CRBC, and requiring suppliers to establish R&D centres and surveillance ports to allow access and monitor of data.[18] These strict requirements potentially could mean that the entire process of IT equipment manufacturing must be restricted to China.

18 For a more detailed analysis on the contents of the CBRC Guidelines see our previous article titled "Made in China or Made for China: CBRC Guidelines Might Bifurcate the Global IT Supply Industry", published in March 2015..

Notably, the CBRC Guidelines was not the first legislation in China where the concept of data localisation was raised. For example, there had been various sector-specific regulations[19] prohibiting or restricting the cross-border transfer of certain data such as State secrets, Personal Financial Information, and health information.

SECURITY UNDER NSL

The later passed NSL comprises of 84 broad, vague and high-level articles with a wide-reaching scope ranging from the economy, to information security, to border control. It defines "national security" to include foreign investments and IT products and services, and imposes a "national security review" regime. Under the NSL, the State shall enhance development of proprietary and "controllable" high-end technology in all fields deemed important by the State. Further, the State shall also construct network and information security protection with the aim of achieving "secure and controllable" systems.

The NSL gives the State the right to gather intelligence information, to conduct risk assessment to review foreign commercial investments, including technologies, internet information technology products and services, as well as other major matters and activities that impact or may impact the national security of China. Moreover, duty is imposed on citizens and enterprises alike, to report any clues and provide evidence as to any "endangering" activities. For enterprises especially, proper education and training is to be provided to its staff members (with April 15th labelled as each year's "National Security Education Day").

RESTRICTIONS UNDER CSL

The draft CSL is the first Chinese regulation exclusively devoted to cyberspace, and covers both security and privacy scope with specific enforcement provisions. It is a single over-arching piece of legislation which seeks to address the collection, storage, transmission and operation of personal information. Although narrowly focusing on cyberspace, the draft CSL also imposes broad reporting duties to the operators of "Critical Information Infrastructures" ("**CII**"), including financial institutions and network service providers. Some duties include conducting background security checks on responsible persons, employing security education and skills assessment for employees, having periodical drills, and putting into place emergency response plans for network security "incidents".

For the first time, network operators are required to obtain consent of the data subject for collecting any information, and data subjects are permitted to request deletion of their personal information upon an occurrence of any data breach. The draft CSL further requires that CIIs store Chinese "citizens' personal data", and "other important data gathered and produced during operations" within mainland China. And any cross-border transfer of such data is prohibited without first undergoing a "security assessment" jointly formulated by the National Cyberspace Administration and State Council. Annual self-inspections of network security are

19 E.g., State Secrets Law (NPC, 1989, 2010) ("secrets in national economic and social development," "secrets concerning science and technology," and even "secrets of political parties"); Notice to Urge Banking Financial Institutions to Protect Personal Financial Information (PBOC, 2011) (identity, property, account, credit, financial transaction, etc); Guidelines for Personal Information Protection within Public and Commercial Services Information Systems (2013), requiring express concern or regulatory approval (voluntary); Administrative Regulation on Credit Information Industry (State Council, 2013), Administrative Measures for Credit Reference Agencies (PBOC, 2013); Anti-terrorism Law (NPC, 2014); Guiding Opinions for Promoting the Innovation and Development of Cloud Computing to Cultivate New Types of Information Industry Services (State Council, 2014); Population Health Information Management (pilot) (National Health and Family Planning Commission, 2014)..

also required, and assessment reports of such to be submitted to the relevant authorities. Note that the data localisation requirement under the draft CSL covers "important data gathered and produced during operations" other than "citizens' personal data" and could potentially govern transactional data resulting in a much broader scope.

The draft CSL clearly stipulates that violation of some of the above requirements may lead to dire consequences, which differs from the broad conceptual language in the NSL. Penalties include suspension of business, take down of websites, revocation of business permits or licenses by the government, and fines between RMB 10,000 to 100,000. Violators of the data localisation rule are subject to higher fines between RMB 50,000 to 500,000 and possibly individual liabilities. At its extreme, the draft CSL even provides power for the government to shut down Internet access in any major "public-security incidents".

TRENDS EMERGING FROM THE SECURITY LAWS

It seems that even though the CBRC Guidelines are currently suspended in its implementation, the core concepts of data localisation permeate and emerge in its own form in the other security laws. In both the NSL and the draft CSL, the phrase "secure and controllable" is repeated throughout the legislation as one of the key objectives. To implement this, the security laws give government authorities to conduct "security reviews" or "security assessments", the standards and criteria of which are unclear.

What is clear, however, is the pattern emerging from the series of security laws released. The CBRC Guidelines are sector-focused on maintaining security with respect to financial institutions; whereas the NSL introduces key ideas which are high-level in nature without specific principles on implementation; the draft CSL is aimed to be much more comprehensive with specific penalty provisions. The passing of the NSL can thus be seen as the security framework upon which more comprehensive, sector-focused rules are to be gradually proposed, giving the government power to enforce any non-compliance, as illustrated in the draft CSL.

COMPLIANCE AND OPERATIONAL CHALLENGES TO FOREIGN COMPANIES IN CHINA

What challenges do these new laws pose to foreign companies which have operations in China? In anticipation of the re-implementation of the CBRC Guidelines (the date of which is not yet confirmed), the China's treatment in dealing with security issues is already seen to be mapped out. Thus, even before formal implementation is underway, foreign companies should adopt strategic measures to address these challenges well in advance:

1. Dealing with data localisation

   The first step to complying with data localisation rules is the identification and subsequent classification of data, i.e., personal information and "other important data" covered by the rules. A feasibility study may be conducted to segregate high-risk data, which may be further protected by encryption and limiting types of services using such data.

2. Combating cross-border data transfer restrictions

   This will arguably be the most challenging aspect resulting from the security laws. The scope and frequency of cross-border transfer, whilst often unclear, must be determined. This is especially important for foreign companies, which will undoubtedly have its headquarters located outside the Chinese territorial borders. Whether transfer of any

transactional data internally (*i.e.*, within the company) constitutes a permanent or "transient" transfer due to technological complexity will need to be ascertained. Thus, foreign companies should consult with data experts to identify all channels of cross-border data transfer possible, and run analyses on the nature, scope, duration and importance of such transfers.

3. Adhering to registration deadlines

   Both the CBRC Guidelines and the draft CSL require submission of plans and reports to certain authorities within unspecified deadlines. As to the actual dates, foreign companies will need to monitor the release of updates and publication of any further guidelines. It is recommended that a team of responsible persons for regulatory requirements be designated, as immediate compliance responses are to be expected once these guidelines are issued.

4. Providing internal training programmes

   Requirements for training are stipulated in both the CBRC Guidelines and the NSL. It is recommended that foreign companies design training programmes on these security laws for their employees, document such training materials, and be prepared to show evidence of records for any training having taken place.

5. Responding to internal procedures and rules

   Foreign companies need to re-assess their internal privacy policies and procedures, for example identifying any reporting obligations, reconsidering data architecture, installing technical measures for any sudden losses of connectivity, and segregating identifiable personal data for deletion requests made by data subjects. Such processes are likely not achievable overnight, and mid to long term planning should commence as early as possible to avoid unintended violation in the future due to delays.

6. Monitoring supply of IT products

   An inventory of domestic and foreign IT products should be kept especially for the financial institutes, with the purpose of maintaining a balanced ratio for smoother transition in the event that some of the CBRC Guidelines are re-issued. Foreign companies are also recommended to be mindful of the origin of their IT products, and conduct feasibility studies of replacing foreign IT products with domestic brands where possible.

CONCLUSION

Given the current social and political backdrop, it appears that tighter security control by the government is an inevitable step for China in the foreseeable future. Although the full implementation is yet to be seen, the issuance of security laws by China so far can provide clues as to the emerging trends, and encourage foreign companies to take adequate practical steps in advance to face such challenges when conducting business in China.

Right to Spend: China's New Draft Online Payment Regulation

By Xiaoyan Zhang, Counsel (New York, USA), Mayer Brown JSM, Hong Kong
June Lau, Trainee Solicitor, Mayer Brown JSM, Hong Kong

On 31 July 2015, the People's Bank of China ("PBOC") released a draft proposal for Administrative Measures for the Online Payment Business of Non-bank Payment Institutions (the "Draft Regulation") for public comment. The Draft Regulation purports to limit the role of non-bank online payment providers ("Payment Institutions," also known as third-party payment providers) in a market totalling RMB 8.08 trillion in 2014 with 50.3 percent of annual growth[20].

The rationale to de-bank third party payment providers stemmed from the inadequate regulation of fund prepayments entering individual consumer accounts that are opened with third party payment providers. In a bid to direct such cash flows out of the prepayment accounts, the Draft Regulation requires a Payment Institution to impose limits to manage the transactions for which an individual consumer makes payment by using the balance of his/her payment account.

Specifically, Article 28 of the Draft Regulation requires that, when an individual consumer makes online payment using the balance of his/her payment account, a Payment Institution shall, based on the security level of the authentication method for payment, impose a cumulative transaction limit payable by a single consumer on a single day. A Payment Institution may adopt combinations of three types of elements[21] to verify a payment instruction by a consumer. For transactions verified with less than two types of elements, the limit shall not exceed RMB 1,000, and the Payment Institution shall undertake to unconditionally bear the liabilities for compensating the risk losses resulting from such transactions. For transactions verified with two or more elements excluding digital certificates or electronic signatures, the limit shall not exceed RMB 5,000.

The proposed daily online transaction limits raised concerns among Chinese consumers who advocated their right to spend. The PBOC argued, however, that imposing such limits would not bring grave inconvenience to consumers because other payment methods such as bank cards and credit cards which do not require a spending limit are readily available. The PBOC also quoted figures showing that 71 percent of consumers made online purchases in 2014 totalling less than RMB 1,000.[22]

20 http://usa.chinadaily.com.cn/epaper/2015-08/04/content_21498684.htm.

21 Article 27 provides for three different types of elements: (1) Elements only known to the client, such as static passwords; (2) Elements that are only held by the client, and are unique, irreplicable or non-reusable, such as digital certificates or electronic signatures that have passed security certification, as well as one-time passwords generated and transmitted through secure channels, etc.; (3) Elements of the physiological characteristics of the client, such as fingerprints.

22 http://www.afr.com/markets/how-chinas-new-online-payment-limit-will-hit-alibabas-alipay-tencents-tenpay-20150805-gislhf?campaign_code=nocode&eid=socialn%3Atwi-140mn0055-optim-nnn%3Anonpaid-27%2F06%2F2014-social_traffic-all-organicpost-nnn-afr-0&promote_channel=social_twitter.

IMPACT ON EXISTING PAYMENT PROVIDERS IN CHINA

Currently there are 269 licensed online payment providers in China[23]. Among them the majority only use one type of verification element such as static passwords and are thus subject to the cap of RMB 1,000 transaction limit per consumer per day under the Draft Regulation.

Alibaba's Alipay and Tencent's Tenpay, with a combined market share of 70 percent in 2014[24], would remain intact from Article 28 of the Draft Regulation. These two online payment provider leaders have made great efforts to evolve from an online payment tool to a comprehensive online finance service provider, including obtaining licences to operate as online banks.[25] On the other hand, the development of smaller online payment firms would be throttled, making it difficult for them to compete in the e-commerce platform under the restrictions set forth in the Draft Regulation.

IMPACT ON PAYPAL

As of July 2015, Paypal is still applying for the license required to operate in China.[26] Once obtaining the license, Paypal will likely qualify as a Payment Institution under the Draft Regulation and payments made via "Paypal Balance" will be subject to the daily transaction limit of RMB 1,000 as long as less than two types of verification elements are used to process online purchases.

PROTECTION TO STATE-OWNED BANKS

Although some believe that the Draft Regulation was an attempt to introduce order into internet finance, others see it as an effort to protect China's State-owned banks. Both views may find support from Article 13 of the Draft Regulation, which prohibits a Payment Institution from providing consumers, directly or indirectly, with cash deposit and withdrawal, credit extension, financing, wealth management, guarantee and currency exchange services — services that are traditionally offered by State-owned banks.[27]

Article 13 would likely have a major impact on products such as Alibaba's Yu E Bao (which allows users to generate interest on the money they deposit in their Alipay wallets), Alipay's credit loan product Huabei (which offers loans between RMB 1,000 and 30,000 for online purchases), and China Mobile's NFC wallets.

CONCLUSION

The online payment business in China has seen a spike in the number of third-party payment providers since the payment business licensing system was established in 2011. Smaller online payment institutions would foreseeably die out under PBOC's efforts to reduce the accumulation of vast money deposits in prepayment accounts.

23 http://news.cnwest.com/content/2015-0811/content_13019842.htm.

24 http://www.redherring.com/internet/tencent-v-alibaba-where-do-they-compete.

25 http://usa.chinadaily.com.cn/epaper/2015-08/04/content_21498684.htm.

26 http://e.tech.163.com/docs/99/2015072211/AV4IoFPM90010FPN.html.

27 http://usa.chinadaily.com.cn/epaper/2015-08/04/content_21498684.htm

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

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

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

ROSITA LI
Partner
+852 2843 4287
rosita.li@mayerbrownjsm.com

XIAOYAN ZHANG
Counsel (New York, USA)
+852 2843 2209
xiaoyan.zhang@mayerbrownjsm.com

NICOLA KUNG
Associate
+852 2843 2261
nicola.kung@mayerbrownjsm.com

Mayer Brown JSM is part of Mayer Brown, a global legal services organisation, advising many of the world's largest companies, including a significant portion of the Fortune 100, FTSE 100, DAX and Hang Seng Index companies and more than half of the world's largest banks. Our legal services include banking and finance; corporate and securities; litigation and dispute resolution; antitrust and competition; employment and benefits; environmental; financial services regulatory and enforcement; government and global trade; intellectual property; real estate; tax; restructuring, bankruptcy and insolvency; and wealth management.

Please visit www.mayerbrownjsm.com for comprehensive contact information for all our offices.