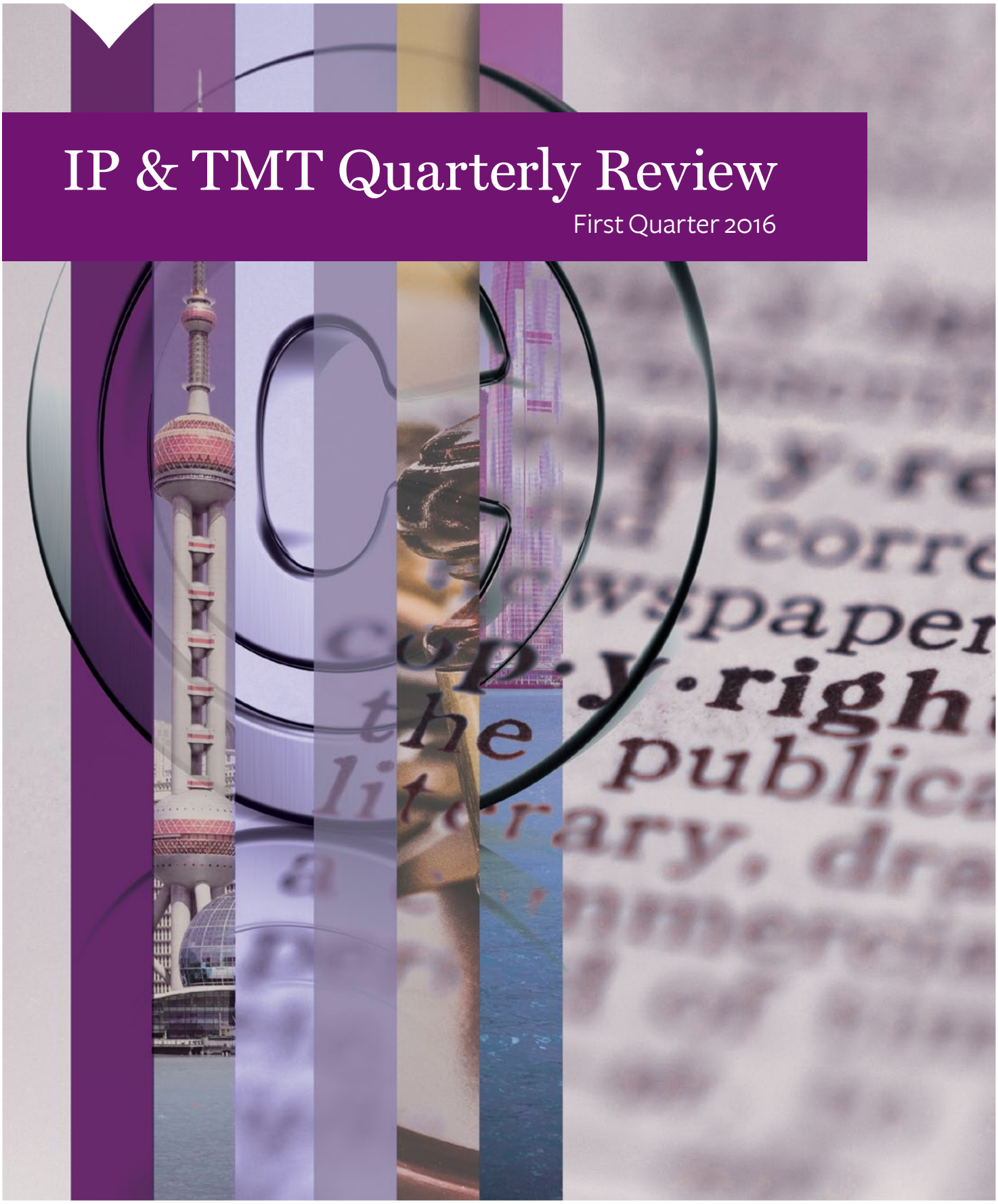
MAYER·BROWN
JSM

IP & TMT Quarterly Review

First Quarter 2016



www.mayerbrownjsm.com

Content

Key: Click to Navigate

TRADE MARKS – HONG KONG

4 Fog Lifting Over the Shadow Company Debate in Hong Kong?

6 Sham Registries and Fraudulent Invoices

7 Tsit Wing Group vs. The Wellness Group: Final Decision on the "TWG" Trade Mark Dispute

TRADE MARKS – CHINA

10 The "PRETUL" case: Manufacturing in China for Overseas Export Insufficient to Constitute Valid Use of Trade Mark

TECHNOLOGY – HONG KONG

13 Sharing is Caring: New Electronic Health Record Sharing System for Hong Kong

DATA PRIVACY

20 Getting Ahead of the Competition? New Tensions Between Competition and Personal Data Revealed

UNFAIR COMPETITION – CHINA

22 China Proposes Amendments to the Anti-Unfair Competition Law

CONTACT US

HONG KONG

Trade Marks

By Gabriela Kennedy, Partner, Mayer Brown JSM, Hong Kong
Amita Kaur, Senior Associate, Mayer Brown JSM, Hong Kong

Fog Lifting Over the Shadow Company Debate in Hong Kong?

The shadow companies saga in Hong Kong has continued for more than 15 years since it started making headlines. Shadow companies are companies incorporated in Hong Kong with a name that is similar to a household brand. They are typically inactive and their directors or shareholders reside overseas, often in mainland China. They will engage the services of a secretarial company in Hong Kong and use that address as their registered address.

For many years, rights holders found it difficult to deal with shadow companies – the two options available either took a long time or were relatively costly and it was difficult to predict the result. The options involved either:

- Complaining to the Companies Registry within 12 months of incorporation of a shadow company on the grounds that the name so adopted is 'too like' the name of an existing company on the register; or
- Commencing civil proceedings in Hong Kong for passing off/trade mark infringement.

The first option was not always successful, while the second left a plaintiff stuck when it came to enforcing an order requesting a defendant to change its name as the Companies Registrar did not have the power to act upon receipt of a court order requiring the defendant to do so. The only effective solution that led to an eventual change of the company name involved joining shareholders of the shadow company as parties to the proceedings and seeking an order from the court that the plaintiff's solicitors be authorised to sign a special resolution on behalf of the shareholders to effect a name change, in the event that they failed to comply. This solution was more costly as it involved service out of the jurisdiction on shareholders located overseas who more often than not provided false addresses.

The 2010 amendment to the Companies Ordinance (Cap. 622) appeared to be the light at the end of a very long and dark tunnel. The amendment empowers the

Companies Registrar to act upon receipt of a court order entering judgment for the plaintiff and requiring the defendant to change its name, if the defendant fails to comply with the order.

However, a recent case in Hong Kong shows that for some plaintiffs and their solicitors, the fog has still not lifted as they are fumbling their way through procedural steps no longer required or appropriate given the 2010 changes to the Companies Ordinance.

In *Jusikhoesa Lock & Lock v Lock&Lock International Brand Management Ltd* [2016] HKEC 516, the plaintiff sought an order empowering its solicitors to pass a special resolution to change the name of the first defendant in the event that the second defendant (the sole shareholder of the first defendant) failed to do so. The court held that it had no jurisdiction to make such an order, as it could not vary the statutory requirements.

However, this request was superfluous as all the plaintiff had to do was to follow the procedure prescribed in Section 108(2) of the Companies Ordinance. This provides that the Companies Registrar may direct a company to change its name if a court makes an order restraining the company from using the name or any part of the name and a sealed copy of the order as well as a notice in the specified form (Form NNC4 – Notice of Court Order Restraining Company from Use of Name) is delivered to the Companies Registrar by a person in whose favour the order was made.

There was thus no apparent need to sue the shareholder (the second defendant, who was the sole shareholder and director of the first defendant) or request an order granting the plaintiff's solicitors the power to sign and file the necessary documents.

We note in passing that the court referred to *Hitatchi Ltd v Hticahi Wei Chu (Hong Kong) Ltd* [2007] 4 HKLRD 431 and the English Court of Appeal judgment in *Halifax Plc v Halifax Repossessions Ltd* [2004] BCC 281. These cases concerned shadow company proceedings where the plaintiffs took action only against the offending company and not also the relevant shareholders. These cases can be distinguished from *Jusikoesa Lock & Lock* primarily because of this fact. The plaintiff's solicitors could not obtain an order empowering them to do something that non-existent defendants did not do.

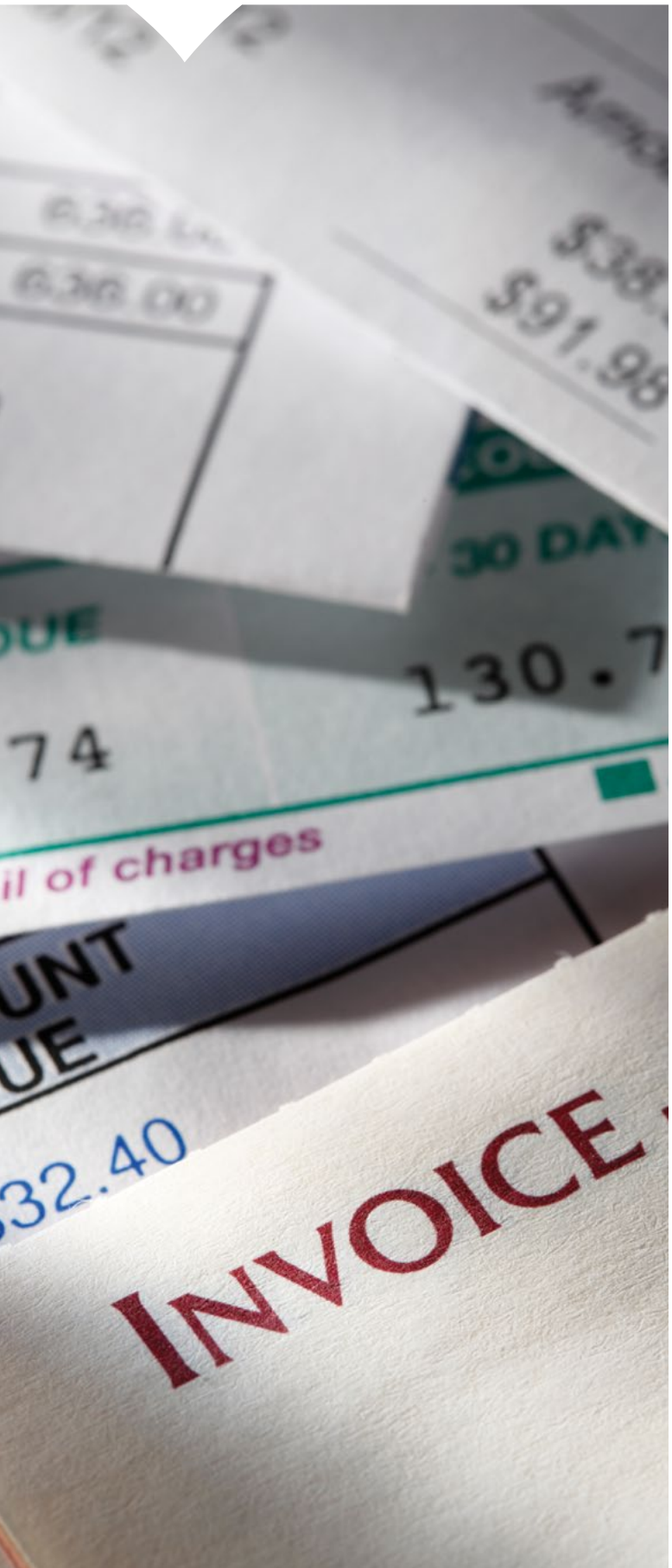
Another factor that troubled the court when confronted with the plaintiff's request in *Jusikoesa Lock & Lock* was that it was not appropriate to allow the plaintiff to choose a new name for the defendant because if the procedure in Section 108(2) were followed, the offending name would be deleted and the new assigned name would be the offending company's registration number.

For now, companies seeking to take action against shadow companies in Hong Kong would be well advised to keep things simple, sue only the shadow company and not also its shareholders and, upon obtaining judgment, follow the beacon of light found in Section 108(2). ◆

HONG KONG

Trade Marks

By Gabriela Kennedy, Partner, Mayer Brown JSM, Hong Kong
Michelle Yee, Senior Associate, Mayer Brown JSM, Hong Kong



Sham Registries and Fraudulent Invoices

In recent years, businesses have become more alert to risks posed by trade mark hijackers and have sought to protect their brands by filing trade mark applications in various jurisdictions around the world. To manage their expanding trade mark portfolios, companies will often engage one law firm to coordinate their global filings and will not be in direct contact with any local agents handling their trade marks in a given jurisdiction. Fraudsters are now taking advantage of this remove by issuing sham invoices directly to applicants for filing and other service fees. In some cases, fraudulent invoices are issued by organisations with names resembling those of official trade mark registries to further mislead recipients. Companies should be vigilant and always check with their service providers before settling invoices from unexpected sources to avoid falling prey to such scams. We have become aware of a few scams concerning CTM filings with sham invoices originating from Eastern Europe. ◆

HONG KONG

Trade Marks

By Rosita Li, Partner, Mayer Brown JSM, Hong Kong
Iris Mok, Associate, Mayer Brown JSM, Hong Kong

Tsit Wing Group vs. The Wellness Group: Final Decision on the "TWG" Trade Mark Dispute

On 29 January 2016, the Hong Kong Court of Final Appeal ("**CFA**") put an end to the 5-year dispute over the "TWG" mark between the Tsit Wing Group ("**Tsit Wing**") and The Wellness Group ("**TWG TEA**"). In its decision, the CFA clarified the Hong Kong position on the law of passing off and also shed light on the approach for determining infringement under section 18(3) of the Trade Marks Ordinance, Cap. 559 ("**TMO**"). Section 18(3) stipulates that "[a] person infringes a registered mark if:

a. He uses in the course of trade or business a sign which is similar to the trade mark in relation to goods or services which are identical or similar to those for which it is registered; ***and***
b. The use of the sign in relation to those goods or services is likely to cause confusion on the part of the public."

Background

Tsit Wing is the successor of a Hong Kong tea business which commenced operation in 1932. In 2006, Tsit Wing registered two marks which contain oval devices and the acronym "TWG", representing the initials of "Tsit Wing Group".

TWG TEA was incorporated in Singapore in 2001. In 2008, TWG TEA adopted the acronym "TWG", standing for "The Wellness Group", as its brand. In December 2011, TWG TEA opened a tea salon at the International Finance Centre in Hong Kong and adopted two marks, namely a cartouche mark with "1837 TWG TEA" and a balloon mark with "TWG TEA" and "PARIS SINGAPORE TEA".

Tsit Wing commenced a High Court action against TWG TEA for trade mark infringement and/or passing off.

Trade Marks Cont'd

The First Instance and Court of Appeal Decisions

Tsit Wing succeeded at trial against TWG TEA on both the passing off claim and the trade mark infringement claim under section 18(3) of the TMO. The decision was upheld by the Court of Appeal (save for a few amendments to certain terms in the injunction order restraining trade mark infringement). In particular, the Court of Appeal held that:

a. In assessing the distinctive and dominant components in a composite mark, generally speaking, words "speak louder" than devices, and there can be more than one dominant feature in a mark. In the present case, the letters "TWG" was at least one dominant feature of Tsit Wing's marks from an average consumer's view; and

b. In assessing the likelihood of confusion, a difference in the colours of the plaintiff's mark and the defendant's sign cannot be used to contend that there is no likelihood of confusion, despite the presence of other similarities. The exclusive right of the plaintiff in respect of the mark embraces its use in whatever colour scheme the plaintiff deems fit.

The Court of Final Appeal Decision

TWG TEA filed a final appeal with the CFA to overturn the judgement issued against it by the Court of Appeal.

THE PASSING OFF CLAIM

To succeed in a passing off claim, a plaintiff has to prove that: (i) it has acquired goodwill in its trade mark; (ii) that the defendant by adopting its sign made a misrepresentation in the course of trade aimed to deceive the public; and (iii) the defendant's action caused damage to the plaintiff.

One of the questions raised by TWG TEA was whether a passing off claim could be sustained by the "mere potential dilution of [the plaintiff's] trade mark". The CFA held:

a. It is well established that the passing off action protects goodwill against its threatened erosion by the activity of the defendant in related fields into which the plaintiff may wish to enter, where that activity causes or is likely to cause deception to those familiar with the plaintiff's mark;

b. The CFA reiterated that there are three interests to be accommodated, namely:

   i. The plaintiff's interest in protecting the "goodwill" flowing from its recognition with customers and prospective customers;

   ii. The defendant's interest in attracting custom[ers] by means it considers effective; and

   iii. The consumers' and potential consumers' interest in selecting goods and services without misrepresentation as to the origin of the defendant's goods or services;

c. If "dilution"[1] by itself was sufficient for an action of passing off, without the need to establish any customer confusion or deception, then it would disturb the balance that needs to be maintained by the courts in respect of the above three interests; and

d. As such, the CFA rejected the expansion of the law of passing off to encompass the concept of "dilution" of the commercial interests of the plaintiff, without consumers being confused or deceived. Such expansion should be a matter of legislative concern rather than a matter for the courts.

However, as the liability of TWG TEA in this case was not determined based on the grounds of "dilution" of Tsit Wing's trade mark. Without confusion and deception, the CFA upheld the lower court's finding of passing off.

1 "Dilution" was described by the trial judge as an unfavourable association likely to be drawn by the public between the plaintiffs and the business of the defendants. The CFA further noted that "dilution" has been used in a different sense in the United States: "the gradual whittling away or dispersion of the identity and hold upon the public mind of the trade mark by its use upon non-competitive goods, which has led to unfair competition by other traders, albeit without the likelihood of consumers being confused or deceived".

THE TRADE MARK INFRINGEMENT CLAIM

TWG TEA also raised the following questions: (i) the correct construction of section 18(3) of the TMO, (ii) whether words speak louder than devices when comparing marks and signs, (iii) the role of colour claims in registered marks and (iv) whether a colour claim affects the distinctive character of a series mark.

In oral submissions for TWG TEA, these questions were somewhat recast into whether the trial judge and the Court of Appeal erred in law: (i) by failing to apply the two limbs of section 18(3) step-by-step; and (ii) when determining the issues of "similarity" and "likelihood of confusion" with regard to the visual and colour elements of the marks.

In answering these questions, the CFA clarified the approach needed to determine infringement of a registered trade mark under section 18(3) of TMO. It held that the court should favour interpretations of a statutory provision which is consistent with international obligations found in Article 16(1) of the 1994 Agreement on Trade-Related Aspects of Intellectual Property Rights ("**TRIPS Agreement**"), and therefore the term "and" in section 18(3) should be employed in a cumulative and causal sense. TWG TEA's appeal on this point failed as they had never argued that the absence of similarity was such that the first limb of section 18 (similarity of marks) was not satisfied. In other words, once the first limb was satisfied, it was not necessary to apply the step-by-step approach.

The CFA further held that when assessing "similarity" under section 18(3) of the TMO, any striking features of the mark or sign which appear "essential" or "dominant" should be considered, without disregarding the entirety of the mark or sign or stripping it of its context, including evidence of what happens in the particular trade. The CFA agreed with the trial judge and the Court of Appeals' approach to the evidence in determining the questions of similarity and likelihood of confusion, and upheld their decisions.

Significance of the Decision

On the law of passing off, the CFA made it clear that the Hong Kong position remains the same, and reinforced the need to accommodate the tripartite interests of plaintiff, defendant and consumer, and refused to expand the law by encompassing the concept of "dilution" of the plaintiff's commercial interests and discard any of the fundamental elements of the tort, such as customer deception. We expect that the courts in Hong Kong will treat with caution any future claims or arguments which require deviation from any of the fundament elements of passing off.

On the claim of trade mark infringement brought under section 18(3) of the TMO, the CFA opined that when it comes to several possible interpretations of a provision of the TMO, an interpretation which is consistent with Hong Kong's obligations under TRIPS Agreement, should be favoured, and that the use of a sign which was likely to cause confusion should be a result of similarity of marks and goods and/or services.

In view of the scarcity of IP cases that go all the way to the CFA, this case provided a golden opportunity for the highest appellate court in Hong Kong to consider and clarify a number of fundamental issues of trade mark law. Although a rare judgement, the CFA missed the opportunity to lay down clear and detailed guidance on pertinent issues, such as the application of the tests of similarity of marks and likelihood of confusion, in addition to the significance of colour claims in trade mark registrations. ◆

CHINA

Trade Marks

By Benjamin Choi, Partner, Mayer Brown JSM, Hong Kong
Cherry Jin, Associate, Mayer Brown JSM, Beijing

The "PRETUL" Case: Manufacturing in China for Overseas Export Insufficient to Constitute Valid Use of Trade Mark

Introduction

A recent decision issued by the Supreme People's Court of China supported the view that the manufacturing of products in China for overseas export purposes does not constitute valid use of a trade mark. Equally, such use cannot be considered an infringement of a trade mark registered in China.

The decision was issued in a case involving the "PRETUL" trade mark with goods produced for export to Mexico. This decision resolves years of uncertainty over the position of Chinese courts, government and Customs authorities over the so-called "OEM" (Original Equipment Manufacturing) principle. Although court decisions in China are non-binding on future cases, judgements from the Supreme People's Court are strongly indicative of possible future trends.

Facts

TRUPER SA is a Mexican company, which holds registered trade mark rights in the "PRETUL" mark and the "PRETUL & oval device" mark in, inter alia, Classes 6 and 8 in different countries, including Mexico. In China, an individual registered the trade mark "PRETUL & oval device" in Class 6 in 2003 and assigned this registered mark to Focker Security Products International Limited ("**Focker**") in 2010.

TRUPER SA entrusted Zhejiang Pujiang Yahuan Locks Co, Ltd ("**Yahuan**") to produce goods bearing the marks "PRETUL" and "PRETUL & oval device" in China. These goods were solely manufactured for export to Mexico.

Focker sued Yahuan for trade mark infringement in the Zhejiang Ningbo Intermediate People's Court (the first

instance court), which ruled in favour of Focker, awarding damages of RMB50,000. Both parties appealed to the Higher People's Court of Zhejiang (the second instance court). The Higher People's Court ordered Yahuan to immediately cease the trade mark infringement and pay Focker RMB80,000. Yahuan filed a further appeal and applied for a retrial at the Supreme People's Court ("**SPC**").

The SPC ruled in favour of Yahuan and revoked the judgments made by the lower courts. The SPC's reasoning was focused on the function of a trade mark as a source indicator. It was held that:

"The primary function of a trade mark under which the Trademark Law intends to protect, is to be a source indicator. When determining whether the act of using an identical/similar trade mark on identical/similar goods is likely to cause confusion, the Court shall base its finding on the trade mark's fulfilment or possible fulfilment as the source indicator. When determining whether trade mark infringement has occurred, the Court should consider whether the trade mark used was able to serve as a source identifier. There is no practical significance in judging that there is a likelihood of confusion when the trade mark involved fails to fulfil its identifying function and therefore does not constitute trade mark use in the sense of the Trademark Law".

Based on the aforementioned reasoning, the SPC ruled that the courts of both instances erred in the application of the law, because they based their assessment of infringement on the sole fact that an identical or similar trade mark was used without authorisation, and ignored the prerequisite that the alleged infringing act must first constitute trade mark use under the Trademark Law. The SPC therefore determined that the use of a China registered trade mark on goods that are manufactured in China solely for export, does not amount to trade mark use and that consequently there could be no finding of trade mark infringement.

Comment

The key element to note in this case is that the trade marked goods were not intended to enter into the China market. Therefore, the action of adding a trade mark onto products is not conventional use of trade mark when such trade marked goods will not be accessed by the public in China. In other words, there will be no risk of confusion in China.

The SPC decision is the latest in a series of court rulings on OEM-related trade mark issues in mainland China. Back in 2004, Nike prevailed in a case in which the Shenzhen court confirmed that the export of goods bearing unauthorized marks constitutes infringement. The defendant was charged with infringement for manufacturing and exporting OEM goods bearing the trade mark NIKE to Spain, even though the mark was registered in Spain by the licensor of the consignee. The court held that because a trade mark registration only afforded local territorial protection, the defendant was not authorized to use the NIKE mark registered in China by the plaintiff who had the exclusive right to that trade mark in China.

In recent years, however, courts in various locations have decided in favour of OEMs, especially in the context of border protection seizures. The Chinese courts and the Chinese Customs have discussed the issues regularly with industry players, but no consensus has been reached.

Back in 2006, the Beijing Supreme People's Court issued an Explanation on Certain Issues Concerning Trade Mark-Related Civil Proceedings imposing a consignee's duty of care as follows:

"when processing products bearing a registered trade mark belonging to another, the consignee should investigate whether the consignor has exclusive right to use that registered trade mark. Where the consignee fails to discharge this duty of care and processes infringing products, the consignee shall be regarded as a joint infringer with the consignor. Such consignee and

Trade Marks Cont'd

consignor shall jointly be liable for damages. If the consignee has no knowledge that such products infringe a registered trade mark and is able to produce the relevant trade mark certificate, he shall not be liable for damages."

This new decision issued by the SPC appears to muddy the waters for brand owners again. To some extent, the exemption for OEMs - at least in certain circumstances - helps companies whose marks are hijacked in China, as it enables them to continue to manufacture products in China and allows their OEM partners to export the products without hindrance. Seasoned brand hijackers in China now also record their trade marks with Customs, and in the past a legitimate foreign brand owner's OEM products risked being seized at the border and/or their Chinese partner being sued for infringement. The SPC decision may now be used by foreign brand owners as supportive evidence to argue for the release by China Customs of OEM products destined for overseas markets.

On the flip side, legitimate brand owners who have registered their trade marks in China, may be unable to prevent an infringer from manufacturing and exporting goods out of China, which bear the brand owner's mark. Brand owners will have to put in more money and effort to investigate the trail of such goods.

Having said that, brand owners should not be disheartened by the SPC decision, especially owners of more notable brand names. The Jiangsu Higher People's Court has decided differently from the SPC in an appeal case in 2015[2]. In that case, the Jiangsu Higher People's Court, though recognizing that the activity involved is OEM manufacturing, ruled that there was infringement because the OEM manufacturer should have known that the Chinese registered trade mark "Dong Feng in Chinese" was a well-known mark and their foreign client may have hijacked the Chinese trade mark and registered the same in the relevant foreign country (though the relevant authority in the foreign country has decided that the registration was valid). This judgment has put the burden on OEM manufacturers to ensure that the company entrusting it with manufacturing has the right to do so.

These cases highlight the intrinsic inconsistency of the Chinese court system, in which the lower courts do not necessarily follow the precedent set by a higher court. Legal precedents have no binding legal effect in China. Whether or not OEM constitutes trade mark infringement remains a complicated issue in China, to be determined on a case-by-case basis depending on numerous factors. It remains to be seen how local courts and administrative trade mark enforcement authorities such as AICs and Customs would be affected by this most recent SPC judgment.

Takeaway Points

In view of this SPC decision, foreign brand owners who have their marks registered in China will need to consider a potential defence of non-infringement available to local OEM manufacturers who deal with their counterfeit goods. Thorough and well-supported investigation can help ascertaining whether the alleged infringing OEM products are solely for export sales and whether the OEM manufacturers have knowledge (or should have knowledge) of the foreign brand involved.

Foreign brand owners should also evaluate if there is actual use of their registered marks in China to ensure they are not exposed to the risk of being cancelled for non-use. The SPC decision can be interpreted to mean use stemming solely from OEM manufacturing does not constitute valid use of a registered mark in China. Foreign brand owners who only manufacture in China, may need to keep re-registering core marks in China on a periodic basis to prevent the risk of non-use cancellation. ◆

2 (2015) Su Zhi Min Zhong Zi No. 00036.

HONG KONG

Technology

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

Sharing is Caring: New Electronic Health Record Sharing System

The ability for doctors, dentists and pharmacists to have quick and ready online access to an individual's medical profile and history (e.g. list of allergies, history of illnesses which may show a pattern indicating a more serious ailment, etc), is a normal expectation in the digital age. Technology nowadays supports the delivery of quality medical services. However, as is always the case with technology – convenience and efficiency must be balanced against the protection of personal data and privacy. As health records contain particularly sensitive information, should they require a higher degree of protection than that afforded to other personal data?

On 2 December 2015, after years of consultation and debate, Electronic Health Record Sharing System Ordinance (Cap. 625) ("**EHRSSO**") came into effect in Hong Kong. The EHRSSO allows healthcare professionals and public and private hospitals to collect, share and store patients' electronic health records via the Electronic Health Record Sharing System ("**eHR System**"). Patients and healthcare providers can join the eHR System on a voluntary basis. The eHR System brings about a major change for private healthcare providers in Hong Kong, most of them operating in small practices and still having paper files and records. The public sector by contrast operates under the Hospital Authority and the Department of Health, which has had in place a well developed electronic data management system for a good few years now, and boasts one of the largest IT workforces in town. The discrepancy between the IT systems for public healthcare vs private healthcare is huge, and investment of time and money will be required from the private health sector to automate their systems in order to be able to register under the EHRSSO.

Technology Cont'd

Health Records = Sensitive Data?

The medical data of an individual generally falls within the scope of "personal data" or "personal information" (i.e. data from which it is practicable to identify an individual), and is protected under applicable data privacy laws. This is the case in many jurisdictions in the Asia-Pacific region.

Some jurisdictions provide a higher threshold of protection for "sensitive data" or "sensitive information", which usually include health records. Australia and Malaysia generally prohibit the collection and use of sensitive information, unless the relevant individual has given his/her explicit consent or one of the exemptions under the legislation apply (for example, where the collection is sanctioned by a court order).

Australia has specific provisions that regulate the handling of health information in its data privacy legislation. Under the Australian Privacy Act 1988 (as amended up to Act No. 157, 2015) ("**Australian Privacy Act**"), "health information" is defined to include "information or an opinion" about "the health, including an illness, disability or injury (at any time), of an individual", "an individual's expressed wishes about the future provisions of health services to the individual", or "a health service provided, or to be provided, to an individual", to the extent that it is also personal information. The Australian Privacy Act specifically allows health information to be collected by an organisation, if it is necessary in order to provide a health service to the individual and the collection is either required or authorised under Australian law.

In contrast, Hong Kong and Singapore data privacy laws do not distinguish between personal data vs sensitive data, nor do they impose more stringent restrictions on the use of sensitive data, over and above the protections applied to personal data in general.

Despite there being no separate category of "sensitive data" under the Hong Kong Personal Data (Privacy) Ordinance ("**PDPO**"), the Hong Kong Privacy Commissioner ("**PC**") tends to take a stricter approach on the application of the Data Protection Principles ("**DPPs**") under the PDPO in respect of personal data that is perceived as being particularly "sensitive", taking into account the nature of the information (e.g. health records, biometric data and Hong Kong identity card numbers) and the context in which it is collected and used.

During the consultation period for the Personal Data (Privacy) (Amendment) Ordinance 2012 (which introduced changes to the PDPO), the Hong Kong Government considered introducing a new category of "sensitive data", which would have been subject to more rigorous controls. However, this proposal was not pursued due to a lack of consensus on the coverage, regulatory model and sanctions for the protection of sensitive data[3]. While the proposal to introduce a new regime to protect "sensitive data" was set aside, the Government asked the Hong Kong Privacy Commissioner ("**PC**") to issue codes and guidelines of best practices on the handling and use of personal data, including health records[4].

Electronic Health Record Sharing System Ordinance

The EHRSSO provides the legal framework for the collection, sharing, use and safeguarding of health records via the eHR System by healthcare providers.

The eHR System has the potential to become an efficient platform for both private and public healthcare providers to share and access patient records. On 13 March 2016, the platform went live, and patients and healthcare providers can now join the eHR System on a voluntary basis. A newly appointed Commissioner for the Electronic Health Record ("**eHR Commissioner**") will oversee the operation and regulation of the eHR System in accordance with the EHRSSO.

3 The Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance issued in October 2010 by the Hong Kong Government: http://www.cmab.gov.hk/doc/issues/PCPO_report_en.pdf

4 Ibid 2.

Hong Kong is not the first Asia Pacific country to launch an electronic health record system. In July 2012, Australia launched its national health record system under the Australian My Health Care Records Act (as amended in November 2015 and formerly known as the Personally Controlled Electronic Health Records Act 2012) ("**Australian Health Records Act**"). Similar to the EHRSSO, the Australian Health Records Act introduced a legislative framework, which allows patients' health records to be shared amongst healthcare providers (unless the patient has not provided her consent or has withdrawn it). The Australian Government is currently running trials in the Nepean Blue Mountains in New South Wales and Northern Queensland. All individuals located in these areas will automatically have a My Health Record created for them, unless they inform the relevant regulator that they wish to opt out. If the trials result in a high adoption rate of the My Health Record system, then the Australian Government may consider switching to a national opt-out scheme from its current opt-in scheme.

In June 2011, Singapore launched its National Electronic Health Record system. All Singapore residents are automatically included in the system, unless they have opted-out. In contrast, Hong Kong has preferred an opt-in system, as individuals must take steps to register and join the eHR System. At the end of 2015, Singapore launched a new online portal and app (known as HealthHub), which allows Singaporean nationals and permanent residents to access their public health records online. Some of the information available is derived from the National Electronic Health Record.

Sharing Health Records – Does it Hurt?

Under the EHRSSO, individuals who register with the eHR System are required to provide two separate consents – their consent to join and participate in the eHR System, and a separate consent to allow the sharing of all their health records with specific healthcare providers ("**Sharing Consent**")[5]. Only healthcare providers to whom an individual has provided their Sharing Consent will be able to access the individual's electronic health record.

Even after an individual's Sharing Consent has been obtained, healthcare providers are still obligated to ensure that access to any health records on the eHR System is only allowed on a need-to-know basis. Healthcare providers must take reasonable steps to ensure that only their relevant staff (i.e. doctors, pharmacists, etc) can access the parts of the health record stored on the eHR System, which are solely needed in order for them to provide the relevant healthcare service to the patient[6]. This will require a lot of discernment on the part of medical staff, and clean categorisation and separation of data. The opportunity for access to more data than needed remains.

The above provisions were agreed by the Legislative Council and were generally non-contentious. During the consultation period for the introduction of the EHRSSO, an area of much debate surrounded the issue of whether or not an individual could restrict the scope within which her data is shared. While the efficient access to electronic health data is the main purpose and benefit of having an eHR System, patients have a reasonable expectation of (data) privacy, and therefore should be entitled to control exactly what data is being shared and with whom.

Given this, it was proposed that instead of individuals only being able to provide an "all or nothing" consent (i.e. consenting to specific healthcare providers accessing all of their medical records pursuant to the Sharing Consent), they should also be allowed to specify certain types of data that would require their further separate consent before such data could be

5 Section 12 of the EHRSSO. Note that a Sharing Consent is deemed to be given to the Department of Health and the Hospital Authority when the patient registers and gives his consent to join the eHR System (Section 16 of EHRSSO).

6 Section 37(2) of the EHRSSO.

Technology Cont'd

accessed (i.e. a "safe deposit box" of information). The downside of allowing individuals to pick and choose what data they shared, is that this might undermine the very objective of the eHR System and render it inoperable.

In the end, due to the sensitive nature of health data, the Government decided to strike a balance between protecting patients' privacy and the overall intent of the eHR System, which is to enable the sharing of such data amongst healthcare providers. In addition to a provision requiring each patient to provide their general Sharing Consent[7], provisions were also introduced that allow an individual to submit a request to restrict the scope of sharing of specific health data [8] ("**Specific Consent**"). The scope of such Specific Consent is to be specified at a later date by the eHR Commissioner. The provisions regarding the Specific Consent are not yet in operation, and are only intended to take effect after a further study and consultation is carried out on how they should be implemented.

eHR System and the PDPO

The EHRSSO and PDPO are intended to be in synch and to achieve the protection of the privacy and security of patients' personal data collected and stored on the eHR System. This means that there will likely be cross-over between the handling of privacy issues between the eHR Commissioner and the PC. For the purposes of the PDPO, both the eHR Commissioner and healthcare providers are considered data users in relation to individuals' health data.

In February 2016, the PC issued two Information Leaflets on the EHRSSO. One was aimed at providing advice to healthcare providers on compliance with the PDPO when using or sharing medical data via the eHR System[9] ("**Healthcare Providers Information Leaflet**"), and the second was aimed at providing practical advice to individuals who are interested in registering with the eHR System[10]. The PC specifically refers to health records as "sensitive personal data" in the Healthcare Providers Information Leaflet, even though the PDPO does not expressly recognise a separate category of sensitive data.

In brief, the Healthcare Providers Information Leaflet advises that:

a. The eHR System is voluntary, and patients must give two consents: (i) to join the eHR System; and (ii) a separate consent to allow their health records to be shared with specific healthcare providers;
b. Patients can withdraw their consent at any time, and healthcare providers must explain the impact of the patient's withdrawal of consent on the heathcare services that they may receive, and how such withdrawal of consent can be made to the eHR Commissioner;
c. Healthcare providers must explain the operation of the eHR System in detail to patients, to ensure they understand the implications on their personal data privacy by sharing their health records;
d. Healthcare providers must ensure that their healthcare professionals only have access to the health records on a need-to-know basis (e.g. setting access restrictions, implementing internal codes dealing with the confidentiality of the health records, etc);
e. Healthcare professionals should exercise their professional judgment to only access the medical data that is necessary in order to provide the relevant healthcare service;
f. Healthcare providers should ensure that the health records are accurate, and only personal data that is necessary and beneficial for the continuity of healthcare should be retained on the eHR System;

7 Section 12 of the EHRSSO.

8 Section 17 and 18 of EHRSSO.

9 Personal Data (Privacy) Ordinance and Electronic Health Record Sharing System (Points to Note for Healthcare Providers and Healthcare Professionals): https://www.pcpd.org.hk/english/data_privacy_law/electronic_health_record_sharing_system/files/eHRSS_Points_to_Notes_ENG.pdf

10 Electronic Health Record Sharing System and Your Personal Data Privacy (10 Privacy Protection Tips): https://www.pcpd.org.hk/english/data_privacy_law/electronic_health_record_sharing_system/files/eHRSS_10_Tips_ENG.pdf

g. Healthcare providers must implement reasonable practicable steps to protect personal data retained on the eHR System;

h. Any data breaches should be promptly notified to the eHR Commissioner and the PC;

i. Use of the personal data contained in the eHR System for direct marketing purposes is a criminal offence, but healthcare providers can still use the personal data stored on their local system for direct marketing, so long as they comply with the PDPO requirements;

j. Healthcare providers should amend their personal data privacy policies to take into account the uploading of patients' personal data onto the eHR System; and

k. If the healthcare provider receives any data access request from a patient in respect of personal data uploaded onto the eHR System by another healthcare provider, then they must inform the patient that their data access request should be referred to the eHR Commissioner.

Offences Under the EHRSSO

In order to give the EHRSSO more "teeth", and to reflect the seriousness of the potential misuse of health records or of any unauthorised access to the eHR System, the Government introduced new offences in the EHRSSO[11].

Under the EHRSSO, a person commits an offence if:

a. She knowingly impairs the operation of the eHR System;

b. She knowingly causes a computer to perform a function so as to obtain unauthorised access to data contained in an electronic health record;

c. She knowingly damages data contained in an electronic health record (without lawful excuse);

d. She knowingly causes access or modification to data contained in an electronic health record, or causes the accessibility, reliability, security or processing of such data to be impaired;

e. She uses or transfers another person's data contained in an electronic health record for direct marketing purposes;

f. With the intent to evade a data access or correction request, she alters, falsifies, conceals or destroys any data contained in an electronic health record; or

g. She makes a false statement for the purposes of enabling a patient to provide his/her consent to the sharing of their data.

Most of the above offences can incur a fine of up to HK$ 100,000 and/or maximum imprisonment of up to 2 or 5 years, save for a breach of the direct marketing prohibition which can result in a maximum fine of up to HK$ 1,000,000 and 5 years imprisonment (which mirrors the penalty for a direct marketing offence under the PDPO).

The offences under the EHRSSO are broader then the related computer crime offences under the Crimes Ordinance (Cap. 200) ("**CO**"), or the direct marketing offences under the PDPO. However, the same acts that give rise to one of the above offences, could also amount to a breach of the PDPO or a crime under the CO, and may come under dual scrutiny of both the PC and eHR Commissioner. If any complaint is issued relating to a breach of the EHRSSO and/or PDPO, then the PC and eHR Commissioner both have the power to refer the complaint to the Police for criminal investigation. The Police can then determine, based on the facts of each case, whether or not it is more appropriate to charge the offender for a crime under the EHRSSO, the PDPO or the CO, or under all of them. In general, the more specific offence applicable to the facts of the case will be invoked and charged by the Police against the offender.

Under Section 161 of the CO, it is an offence to obtain access to a computer in order to commit an offence or with dishonest intent to deceive or cause loss, or to

11 Sections 42 to 47 of the EHRSSO.

Technology Cont'd

make a dishonest gain. While the Government decided to create a more specific computer related offence under the EHRSSO directly in relation to the eHR System, i.e. causing a computer to perform a function in order to obtain unauthorised access to data contained in the eHR System, restricting the scope of the offences to the use of a computer may be limiting, as many other devices, such as a smart phone or tablet, could be used to access the eHR System. Indeed, this is already the case in Singapore where electronic health records can be accessed through the HealthHub app, and health related apps linking patients to healthcare providers in a more de-centralised system are being launched in China.

To allow for future technological developments, further offences were introduced under the EHRSSO, not specifically limited to any means or methods of committing the offence. It is an offence under the EHRSSO to cause any damage or to obtain unauthorised access to the data on the eHR System, or to cause impairment of the accessibility, reliability, security or processing of such data or the operation of the eHR System.

Many healthcare practitioners monetise patients' data by providing it to third parties for medical research or for direct marketing. Under the EHRSSO, extreme caution needs to be exercised by healthcare providers if they decide to disclose patients' personal data to third parties. Whilst the direct marketing offences under the PDPO will only arise if the data user fails to provide the data subject with the required notice and to obtain the data subject's consent, no such procedure applies under the EHRSSO. The EHRSSO makes it an absolute offence for the eHR Commissioner, any healthcare provider or any healthcare professional to use or transfer any of the data contained on the eHR System for direct marketing (even if an individual's consent has been obtained). Unlike the PDPO, this absolute prohibition is not expressly limited to "personal data", but applies to any data or information of a person contained in the electronic health record. This was re-emphasised by the PC in the Healthcare Providers Information Leaflet, thus clarifying that the stricter offence under the EHRSSO would essentially take precedence over the direct marketing provisions under the PDPO.

If healthcare providers have personal data stored on their own local system, the PC has stated that they can still use such personal data for direct marketing purposes, subject to their compliance with the PDPO requirements. However, in practice, it may be difficult for a healthcare provider to prove that it utilised the patient's personal data stored on its own local system, rather than their electronic health records on the eHR System.

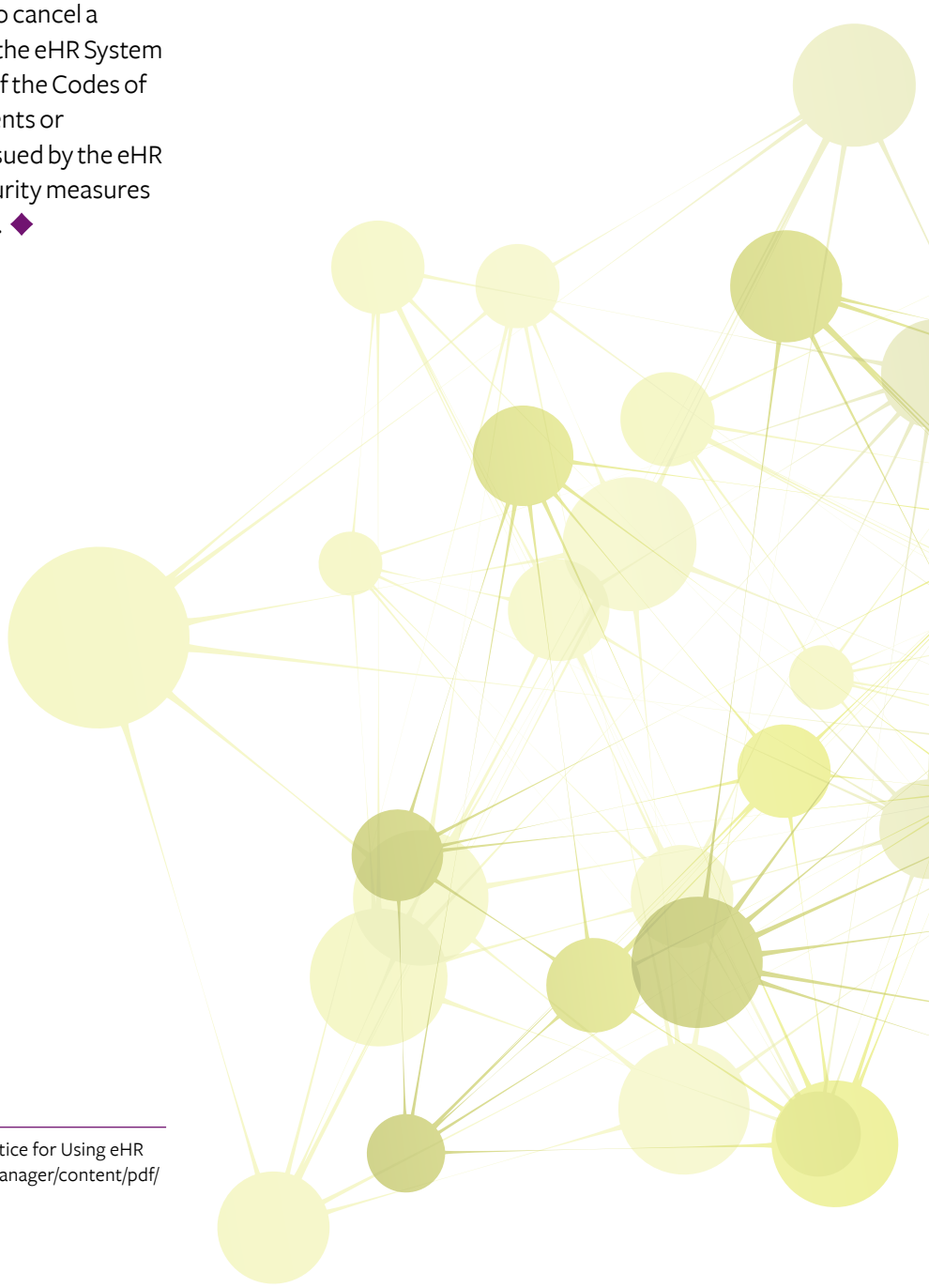
Conclusion

Electronic health records will make the sharing of information easier, and can assist not only with providing better and more efficient medical services to patients, but also assist with medical research and monitoring potential pandemics. Yet greater access, comes with greater vulnerabilities. Cyber security and data hacks make headlines almost on a daily basis, and individuals are more aware and concerned than ever before about their data privacy rights and the security of their data.

The offences introduced by the EHRSSO may act as a deterrent against any misuse of health records or the eHR System, but the EHRSSO provides no specific legal obligation concerning the security measures or safeguards that need to be implemented to prevent cyber hacks. The eHR Commissioner and healthcare providers would still, however, need to comply with the Codes of Practice issued by the eHR Commissioner and the general data security obligation under the PDPO, i.e. to take reasonably practicable steps to ensure the security of personal data and to protect it against any unauthorised or accidental access, processing, erasure, loss or use.

The Codes of Practices that have so far been issued by the eHR Commissioner include a Code of Practice for Healthcare Professionals and Code of Practice for

Management Executives, Administrative and Technical Staff using eHRSS[12], which contain obligations on healthcare providers to implement specific security measures (e.g. maintain security in wireless networks for computers connecting to the eHR System, install appropriate anti-virus software, record and manage access rights, etc). These Codes are not mandatory, but the eHR Commissioner has the power to cancel a healthcare provider's registration with the eHR System if they are found to be in breach of any of the Codes of Practice[13]. We expect further amendments or additional codes and guidelines to be issued by the eHR Commissioner and PC on the exact security measures (including IT safeguards) to be adopted. ◆



12 These Codes collectively form the Code of Practice for Using eHR for Healthcare: http://www.ehealth.gov.hk/filemanager/content/pdf/en/hcp/hcp_code_of_practice.pdf

13 Section 25(1)(a)(ii) of the EHRSSO.

Data Privacy

By Gabriela Kennedy, Partner, Mayer Brown JSM, Hong Kong
Amita Kaur, Senior Associate, Mayer Brown JSM, Hong Kong

Getting Ahead of the Competition? New Tensions Between Competition and Personal Data Revealed

Whereas competition law endeavours to analyse how facts affect price fluctuations and consumer needs, data protection aims to balance an individual's data privacy with the economic aim of enabling the free flow of information.

Extracting value from the personal data collected has become a significant source of power for the biggest players in the Internet sphere.

In a recent case, the German competition authority, the Bundeskartellamt (BKartA) has tapped on this unchartered territory with its investigation of a leading social media company for suspected anti-competitive behaviour stemming from breaches of data protection laws.

BKartA said in its official statement on the probe into a leading US social media company and its Irish and German subsidiaries that there is an initial suspicion that the company's conditions of use are in violation of data privacy laws given the company's dominant position in the market. The company uses different sources to collect a large amount of personal data from users, enabling advertising customers to better target their activities. Data gathered from profiles, friends, postings, activities, and opinions is used for behavioural advertising.

The argument put forward by BKartA is that it is difficult for users to understand the scope of the company's terms and conditions, and there is considerable doubt as to whether this complies with data protection laws. The conduct could also infringe competition rules if BKartA finds a connection between unlawful data protection practice and the company's market dominance.

In response to BKartA's investigation, the French competition authority announced that it does not

intend to initiate a similar probe because it wants to maintain trust and cooperation in the data sector. Instead, the French competition authority would prefer to focus on carrying out a joint study with BKartA on use of data as a competition asset.

There has been criticism levelled on BKartA's investigation with some sectors arguing that competition authorities should not deal with data protection since that would amount to over-regulation whereas their role is to preserve market competition for the benefit of consumers.

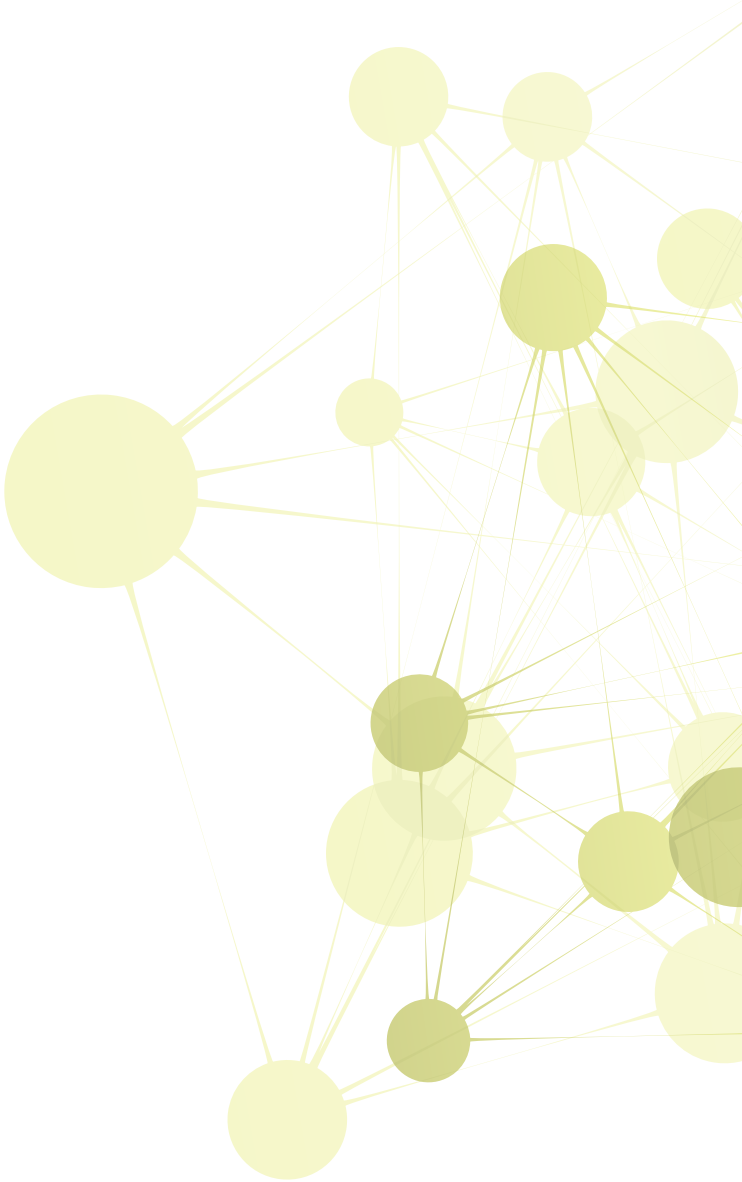
Proponents of the incorporation of privacy into antitrust enforcement argue that the traditional approach to analyzing consumer welfare makes it difficult to regulate major Internet content providers like Google, Facebook, Instagram and Twitter. Most social media, e-mail and search engines are nominally free to consumers and antitrust provisions generally do not address the consumer side of the market when the consumer is not paying for the product or service.

However, some commentators argue that Internet and social media services are not truly free because consumers pay with their privacy.

Because users click boxes to indicate the measure of consent to the privacy terms of the service providers, there is a legitimate concern that the more dominant these companies become over the sectors in which they operate, the less incentive they have to respect a user's privacy.

In the Asia Pacific region where both data privacy and competition regimes are fairly new and developing, would investigations into social media and technology companies in relation to data protection and competition laws be premature?

We expect to see some interest and statements on this new focus of the interplay between data privacy and competition from both data privacy and competition authorities in the region. Guidelines developed by the relevant authorities are likely to follow. ◆



Unfair Competition

By Xiaoyan Zhang, Counsel, Mayer Brown JSM, Hong Kong
Jane Wu, Associate, Mayer Brown JSM, Shanghai

China Proposes Amendments to the Anti-Unfair Competition Law

On 25 February 2016, the Legislative Affairs Office of the State Council released a Draft of the amended Anti-Unfair Competition Law ("**AUCL**") (the "**Draft Amendment**") for public comment. The Draft amends 30 articles out of the 33 articles of the current AUCL in total, removing 7 articles and adding 9. The extensive amendment aims to expand the current scope of unfair competition acts, provide enhanced enforcement measures, and bring the current AUCL in line with the Trademark Law and the Anti-Monopoly Law.

Specifically, the Draft Amendment clarifies six existing unfair competition acts, i.e., market confusion, commercial bribery, trade secret infringement, award promotion, and commercial defamation, and introduces two new acts: the relatively advantageous position and cyber unfair competition. These proposed amendments will have a significant impact on intellectual property, antitrust, and anti-bribery issues.

Market Confusion

Article 5 of the Draft Amendment prohibits the following acts that might cause market confusion:

a. Using identical or similar well-known commercial logos of third parties;
b. Misappropriating registered or well-known marks as business names; and
c. Misappropriating well-known trade names or abbreviations in trade marks or domain names.

This Article now encompasses a broader range of intellectual property related unfair competition acts by expanding the definition of "commercial logo" from product names, packaging, decoration, and names of enterprises to encompass all features that potentially differentiate the product, such as the shape of the product, enterprise's short name, pen name, stage name, website name, domain name, webpage, and

media channel name. This expansion is a significant step towards bringing the AUCL in line with the common law of passing off and the unfair competition laws in other continents.

Administrative Enforcement

Article 3 of the Draft Amendment clarifies that the department of State Administration for Industry and Commerce ("**SAIC**") at or above the county level shall exercise supervision over, and inspection of unfair competition acts. Further, where laws or administrative rules and regulations provide otherwise, relevant departments (such as the General Administration of Quality Supervision, Inspection and Quarantine ("**AQSIQ**"), and Ministry of Culture and Pricing Bureau) may also have supervisory or enforcementpower in .

Article 18 of the Draft Amendment offers improved enforcement measures for acts causing "market confusion". For example, administrative agencies will have the authority to confiscate products, and order parties to change or correct registered company names which cause market confusion. If a sanctioned company refuses to cooperate, or if the illegal income exceeds RMB50K, the agencies have the power to revoke business licenses. The level of monetary fines has been increased to up to five times the amount of the illegal income: no more than RMB250K if the illegal income is less than RMB50K, or between RMB100K and RMB1million if the illegal income cannot be calculated.

Trade Secrets

A new definition of trade secrets is introduced in the Draft Amendment and although the changes to the definition are not major it is easier to prove trade secrets misappropriation as the burden of proof can be shifted to the defendant once the plaintiff establishes a presumption of infringement. The Draft Amendment also increases the maximum administrative fines for trade secret infringement to RMB3 million, compared to the current cap of RMB200K.

Unfair Competition in the Cyber Space

Case law[14] has held that cyber operators who have adopted technical means to influence their users and to interrupt the normal operation of a third party's website are subject to unfair competition regulation. The Draft Amendment codifies the case law by covering the following unfair competition acts in cyber space:

a. Preventing users from using another operators' web services without their permission;
b. Altering a third party's website by inserting links without permission to redirect traffic to its own website;
c. Misleading, deceiving or forcing users to amend, close or uninstall web services legally provided by third parties; and
d. Interrupting or affecting in any way the functionality of a third party's web services.

Relatively Advantageous Position

The Draft Amendment introduces the concept of a "relatively advantageous position", which is a concept that has been used in the PRC administrative regulations[15] as well as under European competition law. If an entity does not have a dominant position in the market, but its trading counterparts depend on that entity or have difficulties switching to other operators, then that entity might be deemed to have a relatively advantageous position. By adopting this concept, the Draft Amendment purports to prohibit acts similar to those regulated by the Anti-Monopoly Law, i.e. imposing unreasonable conditions and restrictions on the trading counterparts' business dealings with third parties, but with a lower threshold than the "dominant market position" requirement.

14 360 v. Tencent, Tencent v.Sogou, Baidu v.Zhu Mu Lang Ma and Baidu v. 3721.

15 Adnmistartive regulations such as Regulations on International Maritime Transportation and Administrative Measures on Fair Trade Between Retailers and Suppliers

Unfair Competition Cont'd

Anti-bribery

The Draft Amendment also expands the definition of commercial bribery to apply to business operators who provide, or offer to provide, financial benefits to a transaction counterpart, or to a third party with power to influence a transaction for the purposes of gaining a competitive advantage. Under this definition, companies may be found liable: (i) if their employees commit acts of commercial bribery; (ii) if a company attempts to conceal evidence of commercial bribery in its records; or (iii) if the act of commercial of bribery is committed by a third party. The penalty for commercial bribery has been raised from the existing range of RMB10K-200K to an amount equivalent to 10-30 percent of the revenue generated by the bribery acts.

Conclusion

If the Draft Amendment is enacted , companies in China should take advantage of the expanded protection and proactively enforce their rights by asserting unfair competition claims concerning commercial logos in particular in cyberspace, and by taking advantage of the increased enforcement powers of administrative agencies. In-house counsel should heed the tightened anti-bribery and trade secrets regulations and take steps to ensure compliance. ◆

Contact Us

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

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

AMITA KAUR
Senior Associate
+852 2843 2579
amita.kaur@mayerbrownjsm.com

MICHELLE YEE
Senior Associate
+852 2843 2558
michelle.yee@mayerbrownjsm.com

CHERRY JIN
Associate
+86 10 6599 9270
cherry.jin@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

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

IRIS MOK
Associate
+852 2843 4263
iris.mok@mayerbrownjsm.com

JANE WU
Associate
+86 21 6032 0234
jane.wu@mayerbrownjsm.com

About Mayer Brown JSM

Mayer Brown JSM is part of Mayer Brown, a global legal services provider, advising clients across the Americas, Asia and Europe. Our geographic strength means we can offer local market knowledge combined with global reach.

We are noted for our commitment to client service and our ability to assist clients with their most complex and demanding legal and business challenges worldwide. We serve many of the world's largest companies, including a significant proportion of the Fortune 100, FTSE 100, CAC 40, DAX, Hang Seng and Nikkei index companies and more than half of the world's largest banks. We provide legal services in areas such as 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.