Fourth Quarter 2015

MAYER·BROWN JSM

IP & TMT Quarterly Review

Table of Contents

Trade Marks – China

Moncler Awarded Highest Amount of Damages Ever for China Trade Mark Infringement

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

BACKGROUND

In 2013 Moncler S.P.A. ("**Moncler**") became aware of the manufacture and sale of down jackets by Beijing Nuoyakate Garment Co., Ltd. ("**Nuoyakate**"). Nuoyakate used marks and logos confusingly similar to Moncler's marks on its products and also applied for the registration of several trademarks and domain names confusingly similar to Moncler's marks in China and other key markets. In November 2014, Moncler brought an action against Nuoyakate for trademark infringement and unfair competition in China's newly established Intellectual Property Court in Beijing ("**IP Court**"). The IP Court awarded Moncler an unprecedented high amount of damages. We look at the reasoning behind this award below.

JUDGMENT

In December 2014, the IP Court issued a judgment against Nuoyakate for trade mark infringement and unfair competition. The IP Court found that Nuoyakate had knowingly and without the trade mark owner's prior authorisation, used trade marks which were confusingly similar to Moncler's trademarks in Nuoyakate's advertisement and promotional activities for the sale of down jackets and accessories. Nuoyakate was also found to have registered the domain name <mockner.com> which was confusingly similar to Moncler's "MONCLER" trade mark.

Nuoyakate was ordered by the IP Court to pay unprecedented maximum statutory damages of RMB 3 million (around US$448,000) to Moncler. The IP Court also ordered Nuoyakate to shut down its website at <mockner.com> and to cease selling clothes that infringed Moncler's trademarks.

Even though Moncler did not produce any evidence of actual loss suffered, and Nuoyakate did not disclose its sales volume or the amount earned by it in relation to the infringing use of Moncler's marks, the IP Court was nevertheless willing to order the maximum statutory damages under the new Trademark Law (effective 1 May 2014). The IP Court's decision was based on the following:

- Moncler had been well-known in the Chinese market since at least 2008;
- Nuoyakate's website to which the domain name <mockner.com> resolved, displayed goods bearing marks that infringed Moncler's trademark rights, which constituted evidence of bad faith;
- Nuoyakate failed to produce evidence to establish its manufacturing volume and revenue made from sales;
- Nuoyakate sold the infringing goods at high prices;
- Nuoyakate deliberately did not print its own company name on the label of the down jackets, which is evidence of malicious infringement; and
- Nuoyakate was a large-scale infringer and in the process of setting up a commercial network including franchising stores and distributors.

ENCOURAGING MESSAGE TO BRAND OWNERS

Moncler is reportedly the first petitioner awarded the maximum statutory damages of RMB 3 million (US$448,000), since the new Trademark Law came into effect in May 2014. Before the new law, the maximum damages available was only RMB 500,000 (US$80,000). As stated by Moncler: "[t]his is a ground-breaking case, believed to be the first judgment under China's new trademark law to grant maximum statutory damages in cases of counterfeiting".

The PRC IP Court is clearly intent on taking a firmer approach to crackdown on the rampant trademark infringement in the country. This landmark case sends an encouraging message to brand owners facing challenges and uncertainties in enforcing their rights through litigation in China.

Trade Marks – Hong Kong

Corinthia Hotels vs. the Residential Property Development Corinthia By The Sea: Can a Hotel Group Prevent the Promotion of a Residential Development in Hong Kong?

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

In *International Hotel Investments plc & Ors v Jet Union Development Limited & Ors* HCA 1941/2015, 3 November 2015 (unreported), the Court considered the Plaintiffs' application for an interlocutory injunction restraining the Defendants from engaging in the mass promotion of a residential development using the English name "Corinthia" on the basis of passing off and trade mark infringement. In the decision, the Court looked at the various elements under the passing off and trade mark infringement claims including misrepresentation and confusion.

BACKGROUND

The Plaintiffs own the "Corinthia" brand and operate the Corinthia Hotel chain which includes Corinthia Hotel London. They brought an action against the developer and manager-to-be of the residential property development "Corinthia By The Sea" ("**the Development**") for trade mark infringement and passing off. The Defendants are beneficially owned by Sino Land Company Limited ("**Sino Land**") and K. Wah International Holdings Limited ("**K. Wah**"), which are joint developers of the Development. Both Sino Land and K. Wah are household names in Hong Kong.

The Defendants registered the "Corinthia" mark in June 2014, and a widely publicised press conference was held in January 2015 to introduce the Development to the public under the Chinese name "帝景湾", the English name "Corinthia By The Sea" ("**the Mark**") and the logo* ("**the Logo**"). A promotion campaign followed, with the Mark and the Logo used alongside the names of Sino Land and K. Wah in all the advertising materials and at the construction site of the Development. Seven months after the press conference, the Plaintiffs brought the action to restrain the Defendants from using the English name "Corinthia" and took out an application for an interlocutory injunction to restrain the defendants from engaging in mass promotion of the Development using the name "Corinthia".

THE INJUNCTION APPLICATION

Applying the *American Cyanamid* principles, the Court must be satisfied that (1) that there are serious issues to be tried; (2) that damages are not an adequate remedy; and (3) that on the balance of convenience, it is just and convenient to grant the injunction.

The passing off claim

To prove a passing off claim, the classic trinity set out in the *Jif Lemon* case, namely, goodwill, misrepresentation and damage, must be present:-

1. *Goodwill*: When considering whether international goodwill of an overseas hotel is recognised in Hong Kong, the hearing Judge, Au-Yeung J, cited the UK Supreme Court decision *Starbucks (HK) Limited v British Sky Broadcasting Group PLC* [2015] ETMR 31 which stated that it would be enough if the Plaintiffs could show that there were people

* 帝景灣 CORINTHIA BY THE SEA

in this jurisdiction who had obtained the right to receive the Plaintiffs' services abroad by booking with an entity in this country. Although the Plaintiffs had engaged an agent to market their hotels in Hong Kong, there was no documentary evidence showing the taking of bookings in Hong Kong. The Judge also noted that any goodwill of the Plaintiffs was limited to the hotel business.

2. *Misrepresentation*: The Judge concluded that there could be no doubt that the Development was that of Sino Land and K. Wah by taking into account features of use of the Mark which distinguish it from the Plaintiffs', including the fact that the marks and logos of Sino Land and K. Wah appear on the construction site and advertising materials in relation to the Development. Further, as the cheapest unit in the Development costs close to HK$ 5 million, an average customer in Hong Kong could reasonably be expected to pay more attention to the details of the developer.

   The Court concluded that there was doubt as to whether there had been misrepresentation.

3. *Damage*: The Plaintiffs complained that the mass advertising by the Defendants was not the typical way any luxury hotel would advertise itself, and would cause damage to the Plaintiffs by tarnishing the distinctive character of their "Corinthia" name. The Judge pointed out that since even the Mandarin Oriental (a luxury hotel group) had engaged in mass advertising by placing advertisements on the outer walls of a public car park in Hong Kong, mass advertising would not necessarily tarnish the status of "Corinthia" as a luxury brand.

THE TRADE MARK INFRINGEMENT CLAIM

The Plaintiffs claimed that "Corinthia" was entitled to protection as a well-known trade mark under the Paris Convention. To succeed in an infringement claim, the Plaintiffs need to show that an identical or similar mark has been used in relation to identical or similar goods or services, which is likely to cause confusion on the part of the public.

When considering whether the Defendants' use of the name "Corinthia" was likely to cause confusion on the part of the public, the Judge confirmed the English Court of Appeal decision in *Specsavers International Healthcare Ltd v Asda Stores Limited* [2012] FSR 19 that the use of the offending sign was to be considered in its context. Applying this contextual approach, the Court ruled that the use of the names, marks and logos of Sino Land and K. Wah in conjunction with "Corinthia By The Sea", "Corinthia" and "帝景灣", would lead an average consumer who is reasonably well-informed, reasonably observant and circumspect to work out that the Development was jointly developed by 2 locally well-known developers, and thus, that such average consumer would not be deceived into thinking that the Development is that of a hotel group.

The Judge concluded that the issues to be tried in both the passing off claim and the trade mark infringement claim fell short of being serious.

THE INTERLOCUTORY INJUNCTION DECISION

Taking into consideration that (i) the Plaintiffs had no goodwill in residential developments in Hong Kong as compared to the established goodwill of the Defendants, (ii) the Plaintiffs failed to show serious issues to be tried, and that (iii) they had delayed in coming to court for an interlocutory injunction: 14 months after the date of Defendants' application for trade mark registration and 7 months after the Defendants' press conference, the Judge refused the application for injunctive relief and awarded costs to the Defendants.

Patents – Hong Kong

Case Update - SNE Engineering Co Ltd v Hsin Chong Construction Co Ltd.

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

On 6 August 2015, the Hong Kong Court of Appeal affirmed a patent decision issued by the Court of First Instance in *SNE Engineering Co Ltd v Hsin Chong Construction Co Ltd*[1]. This case is significant in two material aspects. First, it confirmed the principles applicable to construction of short-term patents and determination of sufficiency and novelty. Second, it clarifies how a short-term patentee can discharge his burden of establishing patent's validity under section 129 of the Patents Ordinance (Cap. 514) (the "**Ordinance**") .

BACKGROUND – SHORT-TERM PATENT

In Hong Kong, there are two types of patents: standard patents and short-term patents, which enjoy a term of protection of 20 years and eight years, respectively. The application for short-term patents is straightforward. Only a request, a specification, an abstract and a search report in relation to the invention are required under section 113 of the Ordinance. Unlike a standard patent, a short-term patent application will not be subject to substantive examination although a short-term patent owner has to establish the validity of his patent before he can enforce his patent rights in court proceedings under section 129 of the Ordinance[2].

FACTS OF THE CASE

Plaintiff SNE Engineering Co Ltd ("**SNE**") was engaged by the 1st Defendant, Hsin Chong Construction Co Ltd ("**Hsin Chong**"), to remove piles at a site for the high speed railway between Hong Kong and Shenzhen. Hsin Chong awarded the contracts to SNE relying on the understanding that the method for removal of piles ("**Method**") had not been used in Hong Kong. SNE then engaged the 2nd Defendant, Chim Kee Machinery Co Ltd ("**Chim Kee**"), to supply machinery and operators for the pile removal works. The works commenced in September 2010.

On 4 August 2011, SNE applied for a short-term patent ("**Patent**") for the Method in Hong Kong. The claims in the Patent were drafted in Chinese and the application was supported by a search report prepared by the State Intellectual Property Office of the People's Republic of China ("**Search Report**"). SNE obtained registration of the Patent on 23 December 2011.

As the pile removal works did not progress at the rate anticipated by the parties, Hsin Chong took over the site in July 2012 and eventually terminated the contracts with SNE. SNE commenced proceedings against Hsin Chong and Chim Kee, contending that Hsin Chong infringed the Patent by using the Method to continue with the works at the site without SNE's permission, and that Chim Kee participated in such infringement by supplying the machinery and operators.

1 [2015] 4 HKLRD 517

2 Section 129 of the Ordinance provides that "In any proceedings before a court for the enforcement of rights conferred under this Ordinance in relation to a short-term patent- (a) it is for the proprietor of the patent to establish the validity of the patent, and the fact that the patent has been granted under this Part shall be of no account in that regard; (b) evidence by the proprietor which is sufficient to establish prima facie the validity of the patent shall in the absence of evidence to the contrary be sufficient proof of such validity."

THE FIRST INSTANCE DECISION

On 26 March 2014, the Court of First Instance rejected SNE's claims and held that the Patent was invalid on two grounds:

a. The specification of the Patent did not disclose the invention in a manner sufficiently clear and complete for it to be performed by a person skilled in the art; and

b. Alternatively, the Method lacked novelty because it had been made available to the public.

In determining whether the Patent should be invalidated on the ground of insufficiency, the Court of First Instance adopted the purposive approach illustrated in *Catnic Components Ltd v Hill & Smith* [1982] RPC 18311 by examining "whether persons with practical knowledge and experience of the kind of work in which the invention was intended to be used, would understand that strict compliance with a particular descriptive word or phrase in a claim was intended by the patentee to be an essential requirement of the invention so that any variant would fall outside the monopoly claimed".[3] Having considered the legal principles and the evidence of the expert witnesses, the Court of First Instance identified a combination of six deficiencies which rendered the patent specification insufficiently clear. For example, the diagrams in the Patent did not correspond with the description of the method in the text and there were technical flaws in the description of the process.

The Court of First Instance then considered how a patentee could discharge the burden of proving the validity of a short-term patent under section 129 of the Ordinance, and held that if the alleged infringer had not put forward evidence to challenge the validity of a short-term patent, then the patent was *prima facie* valid. However, once the alleged infringer had adduced sufficient evidence to challenge the validity of the patent, the burden of proof fell back on the patentee.

The Defendants' challenge against the novelty of the patent based on a product brochure published in Japan failed because the judge found that the method featured in the brochure was not the same as the Method, and even if the methods had been the same, the Method would not be obvious to a person skilled in the art.

The Court of First Instance, however, agreed with Defendants that the Method lacked novelty by reason of disclosure to the public. For example, the Method had entered into the public domain when it was communicated to Defendants by SNE under no duty of confidentiality. The Method has also been disclosed to the public at the site through execution of the works by Chim Kee's operators as a person skilled in the art could derive the Method by reference to what was observable at the site.

ISSUES AT APPEAL

SNE appealed, *inter alia*, the following broad issues:

a. Whether the Patent had been construed properly and whether the Patent was invalid on the ground of insufficient disclosure;

b. Whether the Court of First Instance had interpreted section 129 of the Ordinance correctly; and

c. Whether the Patent was invalid on the ground of lack of novelty due to disclosure before the date of application.

3 Paragraph [109] of the First Instance judgement.

COURT OF APPEAL DECISION

The Court of Appeal considered the Plaintiff's claim on each of the broad issues and dismissed the appeal.

Construction of Patent and Insufficiency

The Court of Appeal held that there was no error of law on the construction of the Patent. The Court of Appeal furthermore found no basis to interfere with the Court of First Instance's ruling of disclosure insufficiency which was a question of fact and degree and an appellate court should be reluctant to interfere with the assessment of evidence by the lower court.

Interpretation of Section 129 of the Ordinance

The Court of Appeal analysed the burden of proof imposed by section129 of the Ordinance in detail, explaining that section 129(a) imposes a legal burden on the patentee to establish the validity of the patent in enforcement proceedings and section 129 (b) imposes an evidential burden to provide *prima facie* evidence of the validity of the patent. It held that the mere fact that the patent had been granted or the mere existence of a search report filed at the time of application would not be sufficient to discharge the evidential burden under section 129(b). Rather, the key question here was "whether the content of the search report is sufficient to support the *prima facie* validity of the patent".[4] If the patentee was able to provide *prima facie* evidence of validity, then in the absence of evidence to the contrary from the defendant, he would meet the burden of proof required by section 129(b).

The lower court found the Search Report insufficient to support the *prima facie* validity of the patent as the description of the Method in the Search Report was inconsistent with the description in the specification of the Patent. The Court of Appeal agreed, noting that the lower court did not adjudicate the invalidity simply because SNE had failed to discharge the burden of proof.

Lack of Novelty

The Court of Appeal endorsed the Court of First Instance's holding that the Method had been made available to the public through disclosures made by Chim Kee's operators at the site prior to the application of the Patent. However, the Court of Appeal disagreed with the lower court's analysis on the question of confidentiality concerning the disclosures made by SNE to Defendants. The Court of Appeal was of the view that the representation by SNE that the method was widely used in Japan was not sufficiently specific to suggest to a reasonable recipient that the Method was already in the public domain in Japan. There was also evidence that the parties viewed their relationship as one of confidence. In light of the conclusions on the other points, the Court of Appeal had left this issue open.

CONCLUSION

In order to discharge the burden of proving a short-term patent's validity under section 129 of the Ordinance in legal proceedings, a patentee will need to show that the content of the search

4 Paragraph [104] of the Court of Appeal judgement.

report is sufficient to support the *prima facie* validity of the patent. Extra care should be given to ensure that the contents of the search report match the description of the specification.

Additionally, to avoid challenges based on lack of novelty, patentees should ensure that adequate confidentiality measures are in place during any commercial dealings prior to the filing of a patent application.

Data Privacy

Blood, Sweat and Tears: Guidance Issued in Hong Kong On the Collection and Use of Biometric Data

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

Face recognition technology to help "tag" friends in photographs, fingerprint recognition to unlock smartphones, and fingerprint door locks are just some of the ways in which biometric data has been used in recent years. The constant barrage of news of cyber-threats, has sparked a renewed interest in biometrics: DNA matching, visual biometrics (retina, iris, ear, face fingerprint, hand geometry), spatial biometrics (finger geometry, hand geometry, signature recognition), auditory biometrics (voice authentication or identification), olfactory biometrics (odour), behavioural biometrics (gait, typing recognition) and biometrics based on brain and heart (drawing on certain brain and heart patterns unique to each individual) are just some of the possible technologies being discussed. In Asia, the uptake of biometric technology includes the development of palm vein authentication technology for payments in Japan, the upcoming introduction in April 2016 in Japan of Biocarts to capture fingerprints and photos of passengers to try and cut down the immigration processing time; fingerprint authentication for ATM transactions in Vietnam; and the launch of facial recognition technology for ATMs in China. Is this the end of long passwords and two-factor authentication systems? Can our memories now take a well-earned break from having to remember frequently changed passwords?

BIOMETRIC DATA – FOR OR AGAINST?

In a consumer context, biometric technology can enhance the users' experience by speeding up delivery and allegedly offering increased security. But is a fingerprint scan more secure than traditional password authentication? Fingerprints can be easily "lifted" and used to fool fingerprint sensors to gain access to a device, as a recent incident involving a German politician has shown us.

Outside of the consumer context, there has been an increased uptake in biometric technology to track employee attendance. Such use gives rise to a host of data privacy concerns, particularly due to the nature of the employer-employee relationship where there is inevitably an unequal balance of power.

Biometrics is also attracting a lot of interest as a tool for stepping up national security in an age of hyper-sensitivity over cyber-attacks and cyber-espionage. The possible introduction of facial matching systems relying on stills rather than live CCTV feeds for use by law enforcement and security agencies has sparked controversy in Australia recently due to a 20% margin of error.

The fact remains that regardless of the benefits of biometrics, the collection of such sensitive data in itself makes the individual vulnerable to a different type of threat, namely misuse, theft, leakage of data or, sometimes, an erosion of human dignity. Unlike passwords, which can be reset when hacked, biometric features when stolen – cannot be replaced.

BIOMETRICS AND THE EVOLUTION OF DATA PRIVACY

Biometric data can be used to identify the individuals from whom it was collected. While such data can be stored on a device or card retained by the individual, the data is also recorded in a central database (many biometric applications have functionalities dependant on such central

databases). Should such data be freely collected and how can data subjects be assured that their biometric data will not be misused? Who has access or who can gain access to the central database recording the biometric data of individuals? The Aadhaar project in India, the most ambitious biometrics database in the world, involves the gathering of fingerprints, iris scans and photos of Indian citizens living in India. The project has been beset by criticism because of the need to counter-balance such an exercise with adequate protection of the individual's privacy; a hard thing to achieve absent any over-arching privacy or data privacy protection in the country.

Yet, the seduction of technology can be giddying: just think of Mastercard's thumbprint biometric card (no more passwords or pins!), Tesco's facial recognition advertising screens (face detection cameras in the screen determine the gender and age of customers and depending on location and time of day allows customisation of ads), apps using facial recognition to authorise payments (an individual's features are his pin for purchases), and eyeball selfie scanning on the phone (eye-recognition technology for personal banking apps on one's smartphone).

It is no surprise that the collection and use of biometric data has led to heightened public and regulatory concern about the risks posed by such practices to data privacy. Most countries, however, do not have specific laws that solely address the collection and use of biometric data, other than general provisions in data privacy laws; a round hole for a square peg.

The data privacy laws of many jurisdictions in Asia-Pacific do not expressly define or clearly refer to biometric data. Instead, biometric data which falls within the definition of "personal data" or "personal information" (e.g., data from which it is practicable to identify an individual) are subject to the existing general data privacy laws.

Some jurisdictions, such as Malaysia and Australia, have additional protections and restrictions regarding the collection and use of "sensitive data" or "sensitive information". Restrictions include a prohibition on collection and use unless the relevant individual has given her explicit consent or one of the exemptions apply (e.g., such use is necessary for medical reasons, etc).

Australia is one of the few jurisdictions that specifically refers to biometric data in its data privacy legislation. Under the Australian Privacy Act 1988 (as amended up to Act No. 62, 2015), "sensitive information" is defined to include "biometric information that is to be used for the purpose of automated biometric verification or biometric identification" and "biometric templates". Biometric information or biometric templates cannot be collected unless the individual has provided his/her consent to the collection, and the information is reasonably necessary for the purposes of a function or activity of the data user. Biometric data cannot be disclosed by the data user for use for any purpose other than one directly related to the original purpose of collection, or only if the relevant individual has expressly consented to the disclosure or the disclosure comes within a specified exemption. Biometric data collected in but transferred outside of Australia, remains subject to the provisions of the Australian Privacy Act 1988, which has extra-territorial effect.

Australia was also the first Asia Pacific jurisdiction to have in place a biometric guideline. In July 2006, the Australian Privacy Commissioner approved the binding nature of the Privacy Code issued by the Biometrics Institute[5], under the sponsorship of the Australian Government.

5 The Biometrics Institute was founded in 2001as an independent and impartial international forum, with the aim of promoting the responsible use of biometrics. The Biometrics Institute has offices in Australia and the UK.

After six years in operation, the Privacy Code, the Privacy Code was revoked in 2012 at the request of the Biometrics Institute due to the changes in technology and the privacy environment since the Privacy Code was drafted.

Hong Kong and Singapore data privacy legislations have no separate definition of sensitive data. In both Hong Kong and Singapore, biometric data would likely fall within the scope of personal data, and be protected under the respective data privacy laws if an individual can be identified from the biometric data itself, or if such data used in conjunction with any other information to which the organisation has access can serve to identify the respective individual.

By contrast, in 2012, the EU Article 29 Working Party[6] issued the Opinion 03/2012 on developments in biometric technology ("**EU Biometric Opinion**"). The purpose of the EU Biometric Opinion was to update the general guidelines and recommendations on the implementation of the data protection principles in relation to biometric data. The Working Party found that most biometric data amounted to personal data, and that its use therefore had to be made in accordance with the data protection principles of the EU Directive 95/46/EC on the protection of personal data ("**Data Protection Directive**"). Once this was established, the EU Biometric Opinion provided unsurprising guidelines, such as that biometric data should only be collected and processed if: (i) informed consent is freely given by the data subject; (ii) the processing is necessary for the performance of a contract to which the data subject is a party, and only where biometric services are being provided; (iii) the processing is required for compliance with a legal obligation; or (iv) where the processing is necessary for the legitimate interests of the data controller, but only if such prevails over the data subjects fundamental rights and freedoms (e.g., to minimise high security risks that cannot be achieved by alternative less invasive measures). Obligations for data controllers to clearly define the purpose for which they collect and process biometric data were included, as were requirements to limit it to what is proportionate and necessary. The EU Biometric Opinion also emphasises the importance of ensuring that data subjects are adequately informed about the key elements of how their biometric data is processed.

In addition to addressing the data users obligations in the context of the Data Protection Directive, the EU Biometric Opinion outlined various types of biometric technology and the specific risks posed by each, as well as technical recommendations aimed at protecting the biometric data being processed.

That was the general landscape as of April 2012. In April 2015, the EU's Court of Justice missed their opportunity in the *Willems*[7] case to require member states to call into question their practices on use and access to a central database of biometric data.

The *Willems* case concerned the EU Regulation[8] requiring Member States to collect and store biometric data (including fingerprints) in passports and other travel documents, for the purposes of verifying the authenticity of the document or the holder's identity. The fundamental question in *Willems* was whether or not the Regulation, together with the Data Protection Directive and the Charter of Fundamental Human Rights, requires Member States to guarantee that any biometric data collected and stored pursuant to the Regulation will not be

6 Article 29 Working Party was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

7 C-446/12 – 449/12 Willems.

8 Council Regulation No 2252/2004/EC

used for other purposes. The EU Court of Justice found that the Regulation did not expressly prohibit the Member States from using the biometric data for any other purpose, and that this issue needed to be determined at national level.

The question of obligations in respect of such biometric data may for now be seen as being sovereign obligations but given recent terrorist attacks in Europe and elsewhere, this question is likely to be revisited before too long.

CLOSER TO HOME – HONG KONG

In Hong Kong, the biggest collector of biometric data is the Hong Kong government. All Hong Kong residents have their finger print data stored on their Hong Kong identity cards. A new smart biometric identity card, for which the Hong Kong government has set aside a whopping budget of HK$2.9 billion, is expected to be introduced in phases between 2018 and 2022. The new smart(er) ID card will store higher resolution images for facial recognition and other enhanced biometric data.

Apart from this, Hong Kong has witnessed an increased adoption and use of biometric technology by the private sector. A few recent instances of misuse of biometric data, raised concerns with the former Hong Kong Privacy Commissioner ("**PC**"), especially in an employment context. On 20 July 2015, the outgoing PC, just days before completing his term in office, issued a Guidance on Collection and Use of Biometric Data ("G**uidance Note**")[9].

Sensitive Data and Biometric Data in the Hong Kong Context

Even before the issuance of the recent Guidance Note, the previous PC tended to take a stricter approach on the application of the Data Protection Principles ("**DPPs**") under the Hong Kong Personal Data (Privacy) Ordinance ("**PDPO**") in respect of personal data that he considered to be "sensitive", taking into account the nature of the information (see various guidance notes and reports of investigations issued and conducted by the PC in the last couple of years). Some examples of personal data that are generally considered to be "sensitive" data, include Hong Kong identity card numbers, medical records and biometric data.

During the consultation period for the Amendment Ordinance 2012 (which introduced changes to the PDPO), the government considered introducing a new category of "sensitive data" (which included biometric data) with more stringent controls attached. Due to a lack of consensus on the coverage and regulatory model for the protection of sensitive data, the proposal was not pursued[10]. We note in passing that many representatives from the information technology sector strongly opposed the proposal lest it would hamper the development of biometric technology[11]. While the proposal to introduce a new regime to protect "sensitive data" and, particularly, biometric data, was set aside, the government suggested that the PC issue guidelines on best practices on the handling of biometric data, in order to afford better protection to individuals[12].

9 https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_biometric_e.pdf

10 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

11 Ibid 2.

12 Ibid 2.

Data Privacy

On 20 July 2015, the Guidance Note[13] was issued in the wake of several cases that raised public concern on the collection of DNA and fingerprints by employers. This was almost the swan song for the former PC before his term finished on 3 August 2015. The Guidance Note replaces the Guidance Note on the Collection of Fingerprint Data issued in May 2012.

BITS OF US: HONG KONG CASES RELATING TO BIOMETRIC DATA

One of the cases that prompted the issuance of the Guidance Note concerns an investment company, which in May 2014 made headlines when it required all female staff to provide blood samples for DNA testing in a misguided attempt to investigate toilet hygiene complaints. On 21 July 2015, the former PC issued an investigation report regarding the collection of employees' fingerprint data by a fashion trading company. In both cases, the former PC found that the collection of such data was excessive, as the sensitive nature of the data was disproportionate to the purpose of collection, and less privacy intrusive measures were available.

In an employer-employee context, even if the collection of biometric data may be justified and proportionate, alternative options should still be provided to the employee (e.g., choice of password access instead of fingerprint scan), otherwise the employees' consent on the collection and use of their biometric data cannot really be said to be voluntary or "fair" for the purposes of the PDPO.

GUIDANCE NOTE

The Guidance Note (which is reminiscent of the EU Biometric Opinion) provides practical guidance to data users on the limited circumstances when biometric data may be collected and, if it can be collected, the steps that need to be taken regarding the collection and storage of such data, namely:

i. Biometric data should only be collected and used in accordance with the relevant data privacy law;
ii. There must be a clear legal purpose for which the biometric data is being collected;
iii. Biometric data must only be collected and used if it is relevant and not excessive in order to achieve such purpose;
iv. An analysis should be conducted to determine whether the proposed biometric technology is essential to and will be effective to achieve the relevant purpose, and whether there are less privacy intrusive alternatives;
v. Sufficient and effective security measures should be implemented to protect the biometric data, taking into account the sensitive nature of the data; and
vi. The data user should establish a retention period, and should ensure that biometric data is deleted once it is no longer needed for the purpose in which it was collected.

The Guidance Note, like the EU Biometric Opinion, goes into further detail and provides practical advice and examples in order to assist data users in their handling of biometric data. In brief, this advice includes the following:

a. Fully inform individuals of the privacy risks and issues involved in the collection of their biometric data, and whether the biometric data may be relied upon to take adverse action against them;

13 https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_biometric_e.pdf

b. Only use and disclose the biometric data for the purposes in which it was originally collected and notified to the data subjects, unless one of the exemptions apply or the explicit consent of the data subject is obtained;

c. Enter into contracts with service providers who receive the biometric data, to ensure that the data is not retained longer than necessary and is kept secure[14];

d. Implement internal policies to ensure that employee-access to the biometric data is restricted and regular training is provided, and take disciplinary actions against any breaches of those policies; and

e. Regular and frequent reviews of the biometric data held by them to ensure that any unnecessary biometric data is purged.

CONCLUSION: NO SWEAT, NO TEARS?

Whilst there are no specific laws in the Asia Pacific region which regulate the collection and use of biometric data, given the increasing adoption of biometric technology, further guidelines and regulations are likely to follow throughout the Asia Pacific region.

Hong Kong is one of the first Asian countries where a regulator has issued specific guidelines on the collection and use of biometric data. Even though the Guidance Note is not legally binding and a breach of its provisions will not in itself constitute an offence, the PC will likely take into account any data users non-compliance with the Guidance Note when determining whether or not there a breach of the PDPO and DPPs has occurred. If after an investigation the PC finds that there has been a breach of the DPPs, it may issue an enforcement notice requiring the data user to take certain remedial action. Failing to comply with an enforcement notice will amount to an offence, resulting in a fine of HK$50,000 and 2 years imprisonment (plus a daily fine of HK$1,000 if the offence continues). However, an even bigger concern for data users is the PC's ability to name-and-shame organisations that have breached the PDPO, which can result in irreperable reputational damage.

Advancements in biometric technology have rendered every day transactions more convenient and more efficient. As more and more "bits" of us are being captured, compressed, encrypted and used to enable daily transactions, what safeguards do we need to have in place, and how will these safeguards differ from one place to another?

The recent *Willems* case in Europe highlighted the confluence of concerns regarding biometric data: data privacy and human rights set against national or international obligations regarding the collection of such data. Add to this mix cyber security concerns and more questions arise.

It seems that in the meantime, more blood, sweat and tears will need to be shed to achieve the elusive balance between improving efficiency and greater security through the use of biometric data, versus safeguarding personal privacy, human dignity and, ironically, the security of such data.

14 DPP 2(3) and DPP 4(a). See also https://www.pcpd.org.hk/english/resources_centre/publications/files/dataprocessors_e.pdf

Data Privacy

Unauthorised Use of Voters' Information

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

It was reported that as of 24 November 2015, the Hong Kong Privacy Commissioner ("**PC**") had received 46 complaints regarding the misuse of personal data during the 22 November 2015 District Council elections. Most of the complaints relate to the unauthorised disclosure or use of voters' information by election candidates and/or their agents. The PC is in the process of making enquiries and will decide whether or not to launch investigations and to issue enforcement notices if it is determined that breaches of the Personal Data (Privacy) Ordinance ("**PDPO**") occurred.

GUIDANCE ON ELECTIONEERING ACTIVITIES

On 25 August 2015, the PC issued a Guidance on Electioneering Activities ("**Guidance Note**") in anticipation of the District Council elections of 22 November 2015. The Guidance Note set out practical advice for election candidates and their agents on how to ensure compliance with the PDPO when carrying out their electioneering activities, e.g., calling or messaging voters to encourage them to vote for a particular candidate. For example, the Guidance Note advised candidates that:

a. They should be directly responsible for ensuring that their campaign staff comply with the PDPO;
b. Only personal data that is necessary and not excessive for carrying out the electioneering activities should be collected (e.g., Hong Kong Identity Card numbers should not be collected);
c. Where the personal data is being collected directly from the individual, such individual should be informed of the purpose for which their personal data is being collected;
d. Personal data should not be collected by deceptive means or by misrepresenting the purpose of collection;
e. With regard to personal data obtained from third party sources (i.e., not collect directly from the relevant individual), the candidate must ensure that the original purpose for which that third party source collected the personal data relates to the intended electioneering activities, otherwise express consent from the individuals will be required;
f. When contacting an individual for electioneering purposes, the candidate (or their agent) should inform the individual of how they obtained his/her personal data when asked; and
g. Individuals should be given an opportunity to decline any further communication regarding the electioneering activities.

CONCLUSION

If the PC decides to conduct a formal investigation and finds that a breach of the PDPO has occurred, then enforcement notices are to be expected. Data protection and data breaches are in the news almost on a daily basis. From misuse of data by financial institutions, to the collection of excessive data through mobile apps, to high-profile data hacks of toy companies which collect data of minors, to data collected in an election context; nothing seems to be out of bounds today when it comes to data privacy.

Technology - China

China's Drones Regulation: Where Is It Headed?

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

On 15 August 2015 and 1 July 2015, China released two announcements[15] ("**Announcements**") regarding export restrictions of Unmanned Aerial Vehicles ("**UAVs**"), commonly known as drones, before they can be approved for export overseas. Both Announcements took effect on the date they were released. The First Announcement requires operators of certain UAVs[16] to make an export application with the Commercial Administrative Department of the State Council ("**Department**") by submitting certain required documents[17]. The Second Announcement governs export controls for three types of UAVs[18] for dual military-and-commercial use.

The Announcements are released with the primary aim of protecting cutting-edge military technology in the interest of national security and concern both military and commercial UAVs. Whereas military UAVs are intended for tactical reconnaissance, carriage of offensive weapons, and projection of surveillance information; commercial UAVs are well-known for their inexpensive and light-weight flying devices whose uses range from aerial photography and site inspection to aerial mapping.

China's move to implement the Announcements is in line with the robust export control regimes endorsed by many countries across the world, notably, the Missile Technology Control Regime ("MTCR") and the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies ("WA").

MISSILE TECHNOLOGY CONTROL REGIME ("MTCR")

The MTCR is a voluntary association of 34 participating countries across the world with the aim of combining national export licensing efforts to prevent proliferation of unmanned delivery systems. It was originally established in 1987 by Canada, France, Germany, Italy, Japan, the United Kingdom and the United States.

15 The two Announcements are: Announcement regarding the Strengthening of Export Controls over Several Dual-Use Items (No. 31 of 2015) released by the Ministry of Commerce and the General Administration of Customs (商务部海关总署公告2015年第31号 关于加强部分两用物项出口管制的公告) and Announcement regarding Export Controls over Unmanned Aerial Vehicles for Dual Military-and-Civil Use (No. 20 of 2015) released by the Ministry of Commerce, the General Administration of Customs, the State Administration of Science and Chinese PLA General Armament Department (中华人民共和国商务部中华人民共和国海关总署国家国防科技工业局中国人民解放军总装备部公告2015年第20号关于对军民两用无人驾驶航空飞行器实施临时出口管制措施的公告).

16 UAVs that are capable of controlled flight outside the natural line of sight of the operator and contain any of the following features shall be subject to export controls: a maximum navigation range equal to or greater than 30 minutes but less than 1 hour and with a maximum wind speed equal to or greater than 46.3 kilometres/hour (25 knots) under the condition of gusty wind; or a maximum navigation range equal to or greater than 1 hour. On the other hand, related equipments or components of UAVs, which enable a UAV to fly at heights of above 15,420 meters (50,000 feet), shall also be subject to export controls under the First Announcement.

17 This includes: identification proof of the legal representative(s), chief manager(s) and the manager(s) of the Applicant; a copy of the contract or agreement; technical notes of relevant items; end-user and end-use assurance; and other documents required by the Department.

18 The three types of UAVs are : (1) a shooting/navigation range equal to or greater than 300 kilometres; (2) capable of an autonomous flight control and navigation capability and include any of the following features: incorporating an aerosol dispensing system or device with a capacity greater than 20 litres; or designed or modified to incorporate an aerosol dispensing system or device with a capacity greater than 20 litres; and (3) capable of controlled flight outside the natural line of sight of the operator and include any one of the following features: incorporating an aerosol dispensing system or device with a capacity greater than 20 litres; or designed or modified to incorporate an aerosol dispensing system or device with a capacity greater than 20 litres.

The MTCR has set out the "*MTCR Guidelines*" and the "*Equipment, Software and Technology Annex*" as guidelines for the implementation of export control legislations within each state. There are two categories of items that are recommended to be subject to export controls, namely, "Category I" and "Category II". UAVs can fall within both categories depending on their technical features. While UAVs in "Category II" are still subject to export restraints, partners shall have greater flexibility in the treatment of "Category II" export applications.

WASSENAAR ARRANGEMENT

The Wassenaar Arrangement ("**WA**") is a well-known international export control regime comprised of 41 participating states and is the successor to the Cold War-era Coordinating Committee for Multilateral Export Controls (COCOM) established in 1996 in Wassenaar, the Netherlands.

UAVs and related components specifically designed or modified for military use shall fall within the "*Munitions List*", whereas those designed to have controlled flight out of the direct natural vision of the operator and consist of certain technical specifications shall fall within the "*List of Dual-Use Goods and Technologies*" under Category 9 (Aerospace and Propulsion). Another important guideline to note under the WA is the "*Introduction to End-User/End-Use Controls for Exports of Military-List Equipment*", which regulates end user/end use controls in the case of exports of military UAVs in order to ensure that exported items will not be diverted to unintended end users or end uses.

RETHINKING CHINA'S POSITION

China is neither a member of the MTCR nor the WA. However, China did apply to be a member of the MTCR back in 2004, but its application was ultimately rejected. The rejection stemmed from the concern that China continued to support other developing countries, such as North Korea, in their development of missile technologies.

Despite not being a member of the MTCR and the WA, China has closely mirrored a number of key export control guidelines set out in the MTCR and the WA in the Announcements. For instance, the technical specifications for UAVs set out in the First Announcement are equivalent to those set out in the "*List of Dual-Use Goods and Technologies*" of the WA. Similarly, the technical specifications for UAVs set out in the Second Announcement are similar to those set out in "Category II" under the MTCR. Notably, the requirement for end-user and end-use assurance under the Announcements is also seen as an important safeguard against unintended use of military UAVs in light of the WA.

The close references to the guidelines under the MTCR and the WA are by no means a coincidence. Given the rising power of China, be it in the political arena or in the drones technology field, the move is clearly seen as a strategic step to cohere with international efforts to procure non-proliferation of unmanned delivery systems commonly endorsed by many countries across the world. While it is hard to predict if China will make use of the Announcements as a breakthrough to the previous rejection by the contracting states of the MTCR, the Announcements will certainly shed positive light on China in view of its tension with a number of Asian neighbors on the issue of military drones development.

Within China, however, the Announcements are still receiving positive feedback as a whole. While the top priority continues to be protecting the national drones manufacturing technology from leaking into unwanted hands, the Announcements ensure that the economic effects

brought by commercial UAVs are not diminished with the implementation of the export controls. For one thing, China has seen an exponential increase in its commercial UAVs exports in recent years. According to Shenzhen Customs District [19], in the first five months of this year, UAVs manufacturers in the city alone exported 160,000 models valued at RMB 750 million (US$120.7 million), a 55-fold increase year-on-year. Of the total, the giant UAV manufacturer in China, Da-Jiang Innovations Science and Technology Company Limited, accounted for more than 95% of sales.

Across the industry, the Announcements have not impacted most commercial UAV manufacturers as their products are often limited to a maximum flight time of about 20 minutes, which will make them naturally fall out of the restrictions set out in the Announcements. Even where the export control restrictions may apply to a number of commercial UAVs manufactures, it appears that the Announcements have not imposed a chilling effect as domestic manufacturers are constantly faced with export control restrictions imposed by other countries, and in most cases, adopt a more robust export control regime than China.

CONCLUSION

The release of the Announcements is a welcome move. While the move sees China coming closer to other contracting states to attain the common goal of non-proliferation of UAVs, it also serves as a mechanism to better protect sensitive military drones technology within the Chinese territory in the interest of national security and at the same time continues to enable its commercial UAVs industry to thrive with few export restrictions. The extent of enforcement of the export control policies in China are yet to be seen, but meantime the Announcements are certainly a positive step forward.

19 See news report entitled "Shenzhen Unmanned Aerial Vehicles Increase Exponentially by Taking Up 99.9% of the Country's Total Exports" (深无人机呈几何级增长占全国出口总量99.9%): http://www.customs.gov.cn/publish/portal109/tab61265/info764080.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
Senior Associate
+852 2843 4452
karen.hf.lee@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

IRIS MOK
Associate
+852 2843 2261
iris.mok@mayerbrownjsm.com

MAGGIE LEE
Legal Assistant
+852 2843 4336
maggie.lee@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.