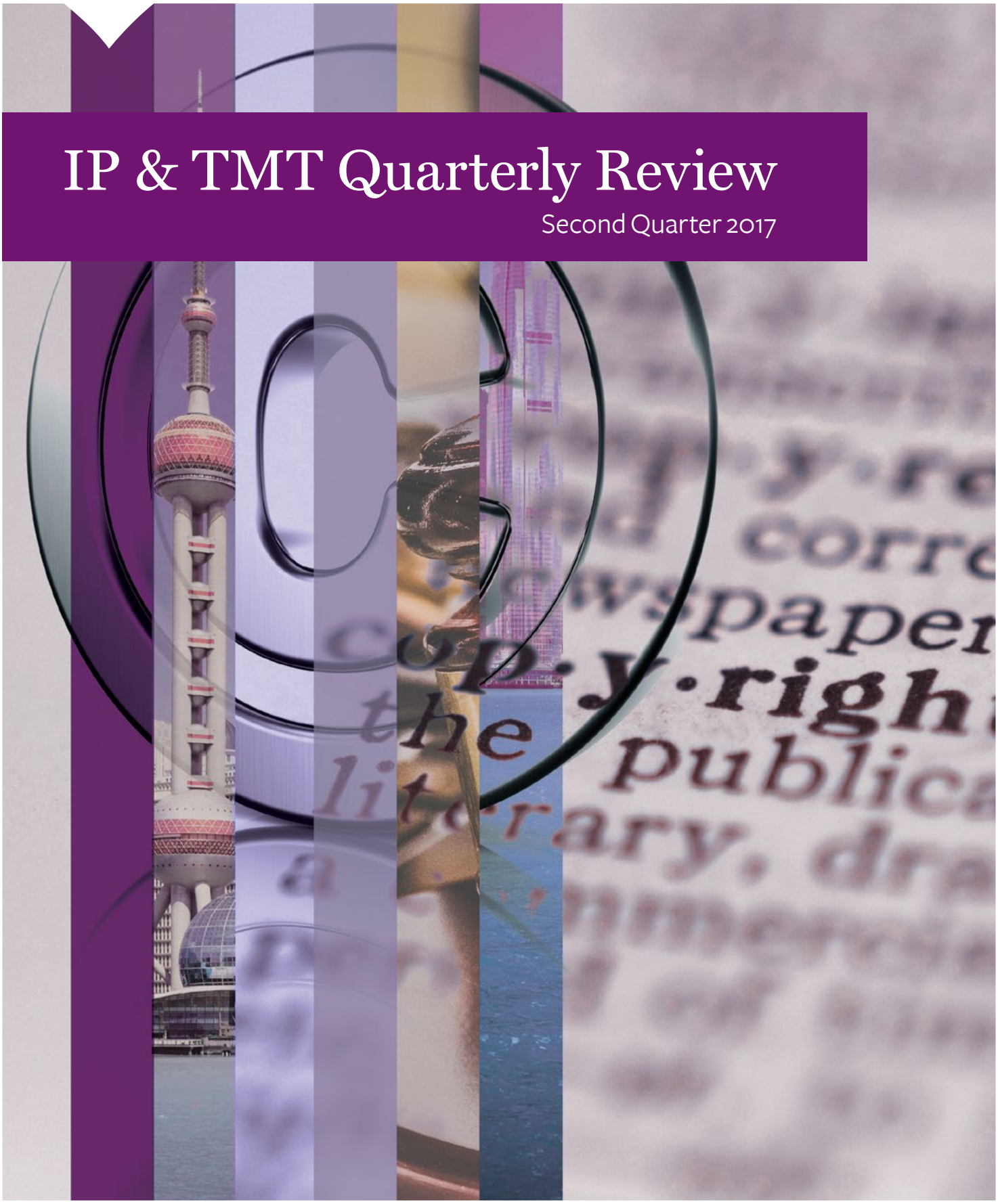
MAYER·BROWN
JSM

IP & TMT Quarterly Review

Second Quarter 2017



www.mayerbrownjsm.com

Content

Key: Click to Navigate

CHINA

Trade Marks

By Benjamin Choi, Partner, Mayer Brown JSM, Hong Kong
Vivian Or, Senior Associate, Mayer Brown JSM, Hong Kong

Beijing IP Court says NO to Trade Marks Filed in Bad Faith

On 24 April 2017, the Beijing Intellectual Property Court ("**Beijing IP Court**") published 18 classic cases concerning trade marks filed in bad faith. The cases are divided into the six categories of: (1) preemptive registration of well-known marks; (2) preemptive registration of marks by agents or representatives; (3) preemptive registration on identical or similar goods of marks already registered; (4) preemptive registration that are detrimental to others' prior rights; (5) hoarding trade marks with no intention to use; and (6) preemptive registration of names of current or past public figures in the political, economic, cultural, religious, ethnic areas etc. The list is a useful guide now for the types of cases where a claim of bad faith would succeed. Two of the cases on the list are discussed below.

Tiffany Case

Tiffany and Company ("**Tiffany**"), a renowned luxury jeweler, prevailed in the invalidation action brought in 2013 against trademark registration no. 8009772 for "蒂凡尼" (pronounced as "Di Fan Ni" in Mandarin) on wallpaper, carpets etc. in Class 27 in the name of Shanghai Zhendi Decoration Materials Co., Ltd. ("**Shanghai Zhendi**").

Unhappy with the decision issued by the Trademark Review and Adjudication Board ("**TRAB**"), Shanghai Zhendi appealed to the Beijing IP Court.

The Beijing IP Court held that Tiffany's "TIFFANY" mark registered in respect of jewellery and precious stones had become well-known prior to the application date of the subject "蒂凡尼" mark. Not only is the "蒂凡尼" mark phonetically similar to "TIFFANY", there is also only one Chinese character difference between Tiffany's Chinese mark and Shanghai Zhendi's Chinese mark "蒂凡尼". The "蒂凡尼" mark therefore constituted an imitation of Tiffany's marks.

Tiffany Case Takeaway

This is a classic case about deterring bad faith registrations under Article 13(2) of the Chinese Trademark Law. In deciding whether the mark concerned would mislead the public and cause detriment to the rights of the well-known trademark owner, the Court

would consider all factors such as the extent of the reputation of the well-known mark, the similarity between the marks, how related the designated goods are, the intention of the owner of the mark concerned, etc. In this case, the extensive and substantial use by Tiffany of the mark "TIFFANY" and of its Chinese mark "蒂芙尼" had resulted in a strong reputation in the market and an immediate correlation of any similar or identical mark to goods associated with Tiffany, namely jewellery. Apart from registering the mark "蒂凡尼", Shanghai Zhendi had also registered the English mark "DIFFANY" and the combination mark "蒂凡尼壁纸 DIFFANY" (essentially "Di Fan Ni Wallpaper DIFFANY") and used the mark "蒂凡尼" together with "DIFFANY". "DIFFANY" is similar to Tiffany's well-known "TIFFANY" mark. Shanghai Zhendi's intention to ride on the reputation of Tiffany's well-known mark could not have been more obvious. The Court considered that the relevant public would likely associate the two marks so that the source of the goods would be mistakenly be attributed to Tiffany and Tiffany's rights would consequently be damaged.

Michael Jackson Case

The last classic case in the Beijing IP Court's list concerns Michael Jackson, the late legendary pop singer. An application for the registration of "MICHAEL JACKSON" as a trademark was made under application no. 8647078 in Class 25 by a party unrelated to the estate of the late Michael Jackson.

DUOFASHION INTERNATIONAL GROUP LIMITED ("**DUOFASHION**") registered the mark "MICHAEL JACKSON" in 2013 and the mark was subsequently assigned to Fujian Fengshang Fashion Co, Ltd. ("**Fujian Fengshang**"). Triumph International, Inc. ("**Triumph International**"), trustee of the estate of late Michael Jackson, filed an Invalidation action against this registration in 2014. Dissatisfied with the decision issued by the TRAB to maintain the registration, Triumph International appealed to the Beijing IP Court.

With the voluminous evidence filed, Triumph International demonstrated that the late Michael Jackson, being a successful pop singer, had an extremely strong reputation and his music made an impact throughout the world. Although the singer passed away in 2009, his name and image have continued to have a substantial economic value. Both Fujian Fengshang and DUOFASHION are unrelated to the late Michael Jackson, it is obvious therefore that by obtaining a registration for "MICHAEL JACKSON" they sought to take advantage of the late singer's worldwide reputation and fame in order to obtain commercial gain for themselves.

Considering the fact that the late Michael Jackson could not take action to protect his own civil rights and the fact that the use of the mark concerned will very likely cause the relevant public to believe that goods or services offered under and by reference to the mark are authorized by or related to the late Michael Jackson, the use of the registered trade mark would likely result in misidentification as to the quality and source of the goods or services and cause damage to the public. The Court decided that in order to protect public interest, the registration should be invalidated as it was contrary to Article 10(1)(8) of the Chinese Trademark Law and constituted "an undue influence".

Michael Jackson Case Takeaway

Chinese law offers no protection over the names of deceased persons, making it difficult for the estate of a deceased person to stop the unauthorized registration of the deceased's name on the basis of personal name rights. The Michael Jackson case shows that in certain circumstances the Court may be prepared to suppress undue preemptive registrations of a deceased person's name as a trademark. As the mark was registered by an entity unrelated to the estate of the late Michael Jackson, apart from possibly causing detriment to the rights of the estate of Michael Jackson, public interest would also be prejudiced by such a misleading registration. The Court's ruling in favour of Triumph International is an encouraging application of the Chinese Trademark Law.

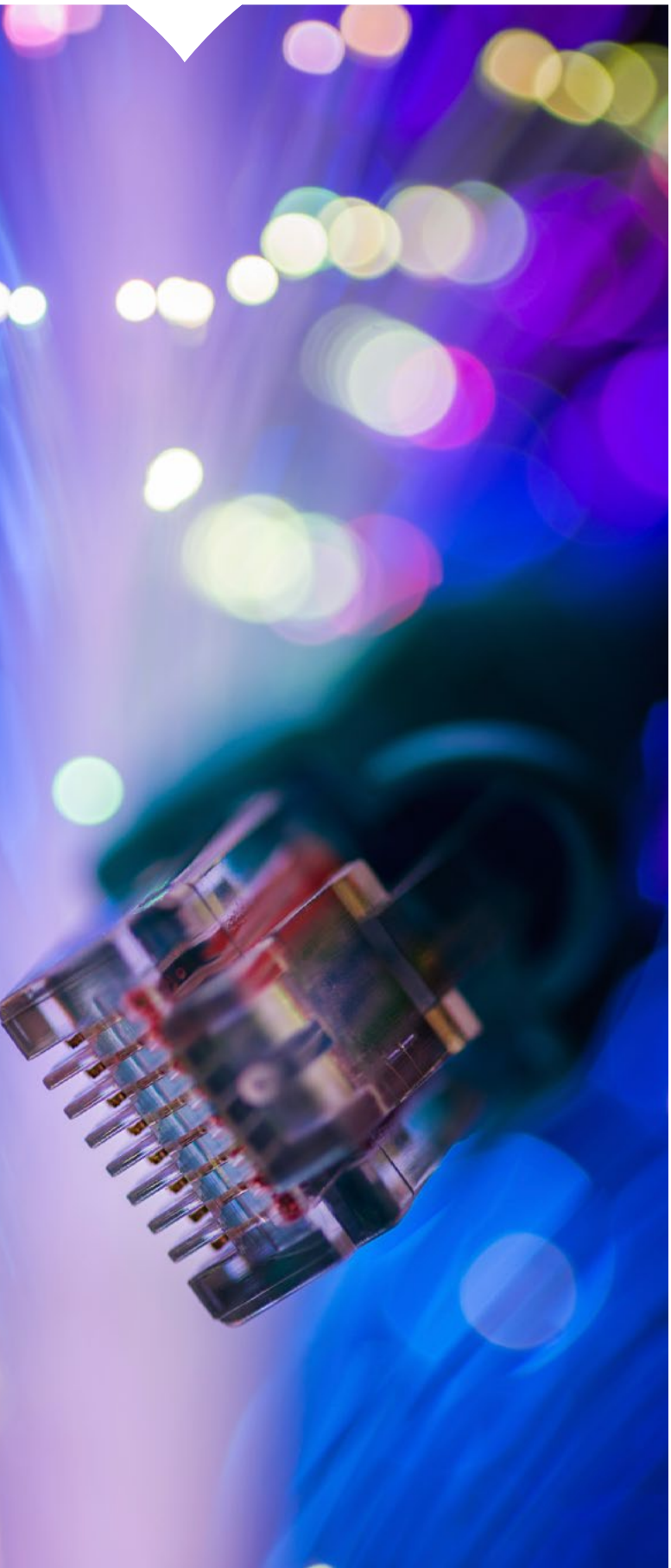
Good News to Brand Owners

These selected cases demonstrate the Chinese Court's determination to reject or invalidate trade marks which amount to acts of copying another's well-known mark in bad faith. Yet this cannot be achieved without the vigilance of the legitimate trademark owners who need to be proactive, and take action as soon as such registrations are detected and be able to adduce satisfactory evidence to support their cases. ◆

HONG KONG

Arbitration

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



New Arbitration Ordinance Amendment Clarifies that IP Disputes are Arbitrable in Hong Kong

Introduction

The Arbitration (Amendment) Ordinance 2017 ("**Amendment Ordinance**") was enacted in Hong Kong on 23 June 2017, bringing about much awaited clarification to the arbitration of intellectual property disputes. Please see here our earlier discussion on the Amendment Ordinance.

Most of the changes brought about by the Amendment Ordinance are due to come into operation on 1 January 2018. The Amendment Ordinance makes it clear that it is not contrary to public policy to enforce arbitral awards involving intellectual property rights.

The Amendments

Intellectual property disputes may be arbitrated[1] and arbitral awards would not be set aside[2], or refused to be enforced[3] merely because the award concerns an intellectual property right. It is clarified that disputes involving intellectual property rights are not incapable of settlement by arbitration, and they do not contravene public policy.

Under the Amendment Ordinance, an intellectual property dispute includes a dispute over the following matters:

a. The enforceability, infringement, subsistence, validity, ownership, scope, duration or any other aspect of an intellectual property right;
b. A transaction in respect of an intellectual property right; and
c. Any compensation payable for an intellectual property right[4].

1 Section 103D of the Amendment.
2 Section 103F of the Amendment.
3 Section 103G of the Amendment.
4 Section 103C of the Amendment.

The term "intellectual property right" is widely and non-exhaustively defined to cover common types of intellectual property rights, including patents, trade marks, designs, copyrights or related rights, domain names, etc., or any other intellectual property rights of whatsoever nature[5]. The types of intellectual property rights set out in the definition are generic, and are not tied to their respective definitions set out in the relevant intellectual property legislation (e.g. the Copyright Ordinance, Trade Mark Ordinance, etc). Such a flexible and broad definition would therefore not only cover all registered and unregistered intellectual property rights subsisting in any part of the world, but also new types of intellectual property rights that may arise in the future.

It has also been clarified that third party licensees do not directly benefit or incur liabilities as a result of arbitral awards involving IP rights unless the third party licensee is joined as a party to the proceedings[6].

Admittedly, arbitration has not been widely used by parties to resolve intellectual property disputes in Hong Kong.

The changes introduced by the Amendment Ordinance would clear the ambiguities of the law relating to intellectual property arbitration, thus promoting arbitration as a means for parties to resolve intellectual property related disputes. The amendments would therefore be very attractive for parties that value confidentiality and speedy dispute resolution, as they are now able to arbitrate intellectual property matters and enforce intellectual property related arbitral awards in Hong Kong.

Are Arbitral Awards Concerning IP Rights Registrable with the Intellectual Property Department?

During the Bills Committee stage, the Bills Committee debated whether arbitral awards concerning intellectual property rights should be registrable with the Intellectual Property Department ("**IPD**"). Some members of the Committee suggested that it may be desirable to allow parties to an arbitration, upon mutual consent, to register their arbitral award or to enter remarks on the register at IPD, thereby allowing the parties to give notice to third parties of the outcome of the arbitration.

It was however emphasized by the Hong Kong government that only matters or documents which have a "towards all effect" (*erga omnes* effect) are registrable with the IPD, e.g. assignments, court orders, etc., and the registration of those matters or documents are governed by specific statutory provisions. Since arbitral awards only affect the rights and liabilities of the parties to an arbitration, it would have little relevance to third parties. As such, the Amendment Ordinance did not include specific statutory provisions for registration of arbitral awards. Should arbitration parties wish to disclose information about the arbitration to third parties, they may still do so, as long as the arbitration parties mutually consent to such disclosure, e.g. by posting information on a party's website.

Conclusion

The Amendment Ordinance coincides with an initiative taken by the Hong Kong International Arbitration Center ("**HKIAC**") to create a pool of arbitrators for intellectual property disputes, so that Hong Kong would be even more attractive to intellectual property rights holders as a seat of arbitration.

With the enactment of the Amendment Ordinance, we remain hopeful that the efforts made by the Hong Kong government and the HKIAC could further advance Hong Kong's position as a global arbitration forum and an intellectual property trading hub. ◆

5 Section 103B of the Amendment.

6 Section 103E(2) of the Amendment.

HONG KONG

Data Privacy

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

Always On Track? The Hong Kong Privacy Commissioner Issues Guidelines on Tracking and Monitoring by Devices

On 11 May 2017, the Hong Kong Privacy Commissioner ("**PC**") issued a new Information Leaflet on Physical Tracking and Monitoring Through Electronic Devices ("**Information Leaflet**"). The Information Leaflet provides operators and manufacturers of electronic devices with practical advice on how to ensure compliance with the Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**").

Background

Internet of Things ("**IoT**") devices provide efficient solutions and methods of tracking and gathering data and other information (e.g. monitoring the contents of your fridge, keeping track of your belongings, recording the number of steps you have taken and tracking your sleep patterns). Common features of IoT devices include the ability to track physical locations and monitor individual behaviour (e.g. through the use of Wi-Fi transmitters or radio frequency identification ("**RFID**") tags). Given the ever increasing popularity of IoT devices, it is inevitable that privacy concerns should arise considering the amount of personal data being collected through such devices. Many users may be unaware that their movements or behaviour are being tracked by their IoT devices, and even fewer are aware how such data may be used. Is it being used to build their profile (e.g. their personal preferences, daily activities, shopping habits, etc) and, if so, how is this profile going to be used in the future? Can the individual concerned review it or have a say regarding its further use?

On 24 January 2017, the PC issued the results of a study on fitness bands and their related mobile applications ("**Study**"). The Study was carried out as part of the 2016 Global Privacy Enforcement Network Sweep ("**Global Sweep**"), which concerned the collection and use of personal data by IoT devices – 25 privacy enforcement authorities (including those in Hong Kong, Canada, the UK and Australia) participated in the Global Sweep. The

Global Sweep revealed a general lack of transparency in respect of privacy practices and security safeguards by IoT device manufacturers[7].

Spurred on by the results of the Study and the Global Sweep, the PC has issued the Information Leaflet as a first step towards tackling the privacy concerns identified in relation to IoT devices.

Information Leaflet

If the identity of an individual can be directly or indirectly ascertained based on the data being collected by any electronic device that monitors behaviour or tracks physical locations, e.g. IoT devices ("**Devices**"), then this will amount to personal data that is subject to protection under the PDPO and the Information Leaflet. Even data which by itself may appear to be anonymous (e.g. GPS location data), may still amount to personal data if an individual can be identified when such data is combined with other information held by or accessible to the Device operator.

Prior to launching a Device, operators must first carry out a privacy impact assessment ("**PIA**")[8]. The overall aim of the PIA is to reduce the extent and sensitive nature of the data being collected by the Devices; reduce the privacy risks to which individuals are exposed; and provide transparency in order to minimise any surprises to the relevant individuals. The PIA will help Device operators identify and detect any potential privacy issues from the outset, and to address them prior to launch.

Even if the data being collected is not capable of identifying an individual user, the user may still perceive the Device as collecting and using their data in a manner that violates their privacy. For example, targeted advertising based on anonymous profile information. Therefore, the PC recommends that the PIA should be carried out bearing in mind the potential user perceptions in relation to their privacy.

When carrying out the PIA, the Device operators should:

a. Assess each type of data being collected to determine whether or not it is necessary, and whether the collection of such data can be minimised whilst still achieving the same purpose;
b. Assess whether or not the Device operator is transparent with individual users about how their data is being tracked and monitored, and allow the individuals to opt-out where possible;
c. Identify any privacy concerns and implement controls or remedial actions to deal with them; and
d. Keep a record of the PIA analysis carried out, so that the Device operator can rely on it in the event of any investigation or enquiry by the PC.

Manufacturers of Devices are strongly advised by the PC to adopt a "privacy by design" approach. For example, minimising the amount of data being collected to what is essential and implementing default settings that are the least privacy-intrusive.

In addition to the above, the Information Leaflet also provides the following recommendations:

1. Device operators must be transparent about how they will use the location or behavioural data collected. Individual users of the Device must be informed beforehand, in clear and simple language, about the location or behavioural data which will be collected and the purpose of collection. If the tracking or monitoring features of the Device are not essential to the main function of the Device, then individual users must be notified that they can opt-out and should be provided with an easy mechanism in order to exercise such opt-out rights. If such features are compulsory, then the individual users must be informed of the consequences if they do not want their movements or behaviour to be tracked (e.g. the Device cannot properly function, etc).

7 For further details on the Study and the Global Sweep, see our article entitled "IoT (I Own Thee): Hong Kong Releases Results of Study on Wearable Technology Devices": https://www.mayerbrown.com/files/Publication/98f5a31d-b5f1-4333-abb4-db11fefdf564/Presentation/PublicationAttachment/90274712-8db3-419a-a123-c128c4da060b/170323-ASI-IP-TMT-QuarterlyReview-2017Q1.pdf

8 See the PC's Information Leaflet on Privacy Impact Assessments issued in October 2015: https://www.pcpd.org.hk//english/resources_centre/publications/files/InfoLeaflet_PIA_ENG_web.pdf

Data Privacy Cont'd

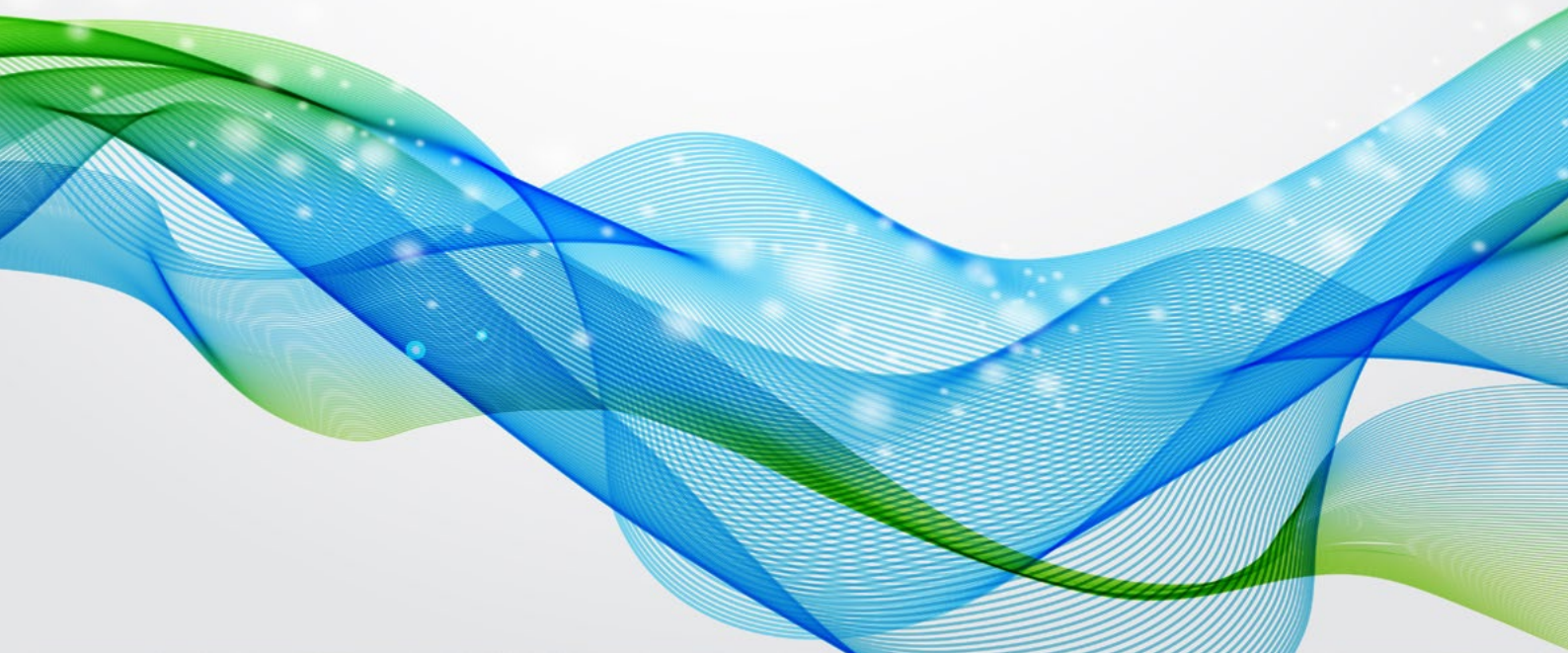
2. If any tracking or monitoring will be carried out for direct marketing purposes (e.g. to send targeted marketing materials to users based on the data collected), then this cannot be done without the individual users' prior consent. The PDPO has stringent requirements on the collection, use and transfer of personal data for direct marketing purposes and such requirements will equally apply to any Devices. For example, if a Device tracks an individual user's preferences in terms of routes for jogging, then using that data to send direct marketing emails addressed to that individual on breakfast offers at restaurants along that route would require the individual user's prior consent. In addition, no such data may be transferred to a third party for them to send direct marketing materials to the relevant individual, unless their prior written consent has been obtained.
3. Device operators should ensure that no personal data is kept longer than necessary to fulfil the purpose of collection (or a directly related purpose). All practicable steps should also be taken to ensure that the personal data collected is accurate before it is used. This is especially important if adverse consequences may occur or adverse inferences may be drawn in relation to the data. For example, the individual users should be allowed to provide comments before their data is used in any adverse manner.
4. The personal data collected via the Device should only be used for the purpose (or a directly related purpose) for which it was originally collected, as notified to the individual user on or before the collection of their data. If the Device operator would like to use it for any new purpose, then it must obtain the prior express consent of the relevant individual.
5. Device operators should implement an appropriate level of encryption to protect the data collected, both during transmission and storage. Internal measures must also be adopted to prevent any unauthorised access of the data by employees or third parties.
6. Individual users should be clearly informed of the Device operators general policies and practices when handling personal data, and practicable steps should

be taken to ensure that they are properly brought to the individual users' attention.

7. Mechanisms should be put in place to enable individual users to request access to and to correct their personal data held by the Device operators.
8. Manufacturers of the Devices should adopt mechanisms that prevent the movement of users from being tracked without their knowledge.
9. Mobile app users should be given the option to decide whether or not an app can have access to their location data.
10. Individual users should be clearly informed on how they can delete their personal data stored on the Device and remotely.
11. Individual users should be provided with the contact information of the relevant Device operator or manufacturer to whom it can address any privacy related concerns.
12. Manufacturers of Devices must implement mechanisms so that the Device cannot collect or record any data (e.g. through sensors, etc) without the individual user's conscious activation and knowledge.
13. Manufacturers of Devices should ensure that no scanners can read any unique identification information linked to a Device without the individual users' knowledge, so as to prevent any covert tracking.
14. If any Device can collect data of another individual, who is not the user of the Device, then sufficient warning needs to be provided to such individuals and the user.
15. Where RFID tags are used, individuals should have the right to opt-out of them being included in any products they purchase, and must be clearly informed of any RFID tags embedded in a product. Personal data should not be stored on any RFID tags in so far as is possible. If personal data must be stored on an RFID tag (e.g. because it is the primary function of it), then the PDPO must be complied with.

Takeaways

The PC has sharpened his focus on IoT devices. Operators should start carrying out PIAs and assess their privacy procedures, in order to promptly resolve any shortcomings or risks that they identify. Consumers in Hong Kong are becoming increasingly savvy with regard to their privacy rights. With the PC's attention firmly on IoT devices, enforcement actions are expected in the future. The reputational damage that can occur as a result of an enforcement action may derail the best business plans for new IoT devices. ◆



HONG KONG

Data Privacy

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

The Pitfalls of Networking: Individual's Conviction Upheld for Transferring Personal Data for Direct Marketing Purposes

On 2 June 2017, the Court of First Instance ("**CFI**") upheld the conviction of the Eastern Magistrates' Court against an individual, for breach of the direct marketing provisions under the Personal Data (Privacy) Ordinance ("**PDPO**").

Restrictions on Transfer

Under the PDPO, a data user cannot transfer an individual's personal data to a third party for their use in direct marketing, unless the prior written consent of the individual has been obtained. Any such consent will only be valid if the data user has notified the individual of the following:

a. That it intends to transfer the individual's personal data to a third party for direct marketing purposes, and cannot do so without their consent;
b. The classes of recipients to whom their personal data will be transferred;
c. The type of personal data that will be transferred;
d. The classes of goods, facilities or services that will be marketed by the third party recipient;
e. Whether the personal data is being transferred in return for gain (e.g. in return for payment, etc); and
f. A response channel through which the individual can communicate their consent in writing (without charge).

Breach of the direct marketing restrictions amounts to a criminal offence and can incur a hefty fine, the maximum of which is HK$1,000,000 and up to 5 years imprisonment (depending on the gravity and nature of the breach).

The Case

During a social function, the defendant had collected the name and phone number of an individual ("**Complainant**"). The defendant subsequently

transferred the Complainant's personal data to an insurance agent, without notifying or obtaining the Complainant's consent prior to the transfer of the personal data.

The insurance agent called the Complainant, identifying herself as a financial planner of an insurance company, and informed the Complainant that the defendant had provided her with the Complainant's name and phone number. The Complainant ended the call when he realised that the insurance agent was calling for the purposes of promoting financial planning and insurance products.

In April 2014, the Complainant issued a complaint to the Hong Kong Office of the Privacy Commissioner of Personal Data ("**PCPD**"). The PCPD subsequently referred the matter for prosecution and the case was brought before the Eastern Magistrates' Court. The defendant was found to have committed an offence under Section 35J of the PDPO as a result of him transferring the Personal Data to the insurance agent without the Complainant's consent, and was ordered to pay a fine of HK$5,000.

The defendant appealed the Magistrate's decision. The CFI upheld the lower court's finding that the defendant's act of sharing the Complainant's personal data with the insurance agent, without obtaining his prior consent, knowing that the insurance agent may use the data to try and sell insurance products, amounted to a breach of the PDPO. Whether the insurance agent had actually ended up using the personal data for direct marketing purposes was irrelevant. The CFI also confirmed that the word "offer" in the context of the definition of direct marketing under the PDPO, should be interpreted broadly so as to include mere acts of suggesting or alluding to the possibility of providing a product or a service. This would therefore capture direct-marketing communications that ended at an early stage, due to the data subject expressing his lack of interest at the outset in the product or service being marketed.

A number of decisions issued at Magistrate Court level have gone on appeal to the CFI. So far, the High Court has upheld the decisions of the lower courts in relation to direct marketing convictions under the PDPO. On 27 January 2017, the High Court upheld the Tsuen Wan Magistrates' Court's landmark conviction of 2015 in which the internet service provider, Hong Kong Broadband Network Limited ("**HKBN**"), was fined HK$30,000 for breach of the direct marketing provisions[9].

Individuals as Data Users

The recent decision draws attention to the fact that individuals as data users are subject to the PDPO if they collect and use personal data, just like a data user that is a corporate body. Given the ubiquitous collection of data through apps, it appears that the spotlight is now shifting to individuals as data users. The PCPD has raised recent concerns in relation to individual app users who have allowed apps to collect personal data stored in their phone books on their mobile device.

In May 2017, it was found that an app known as DU Caller, had been collecting and using personal information without the knowledge or consent of relevant data subjects. Whilst DU Caller allows users to filter and block unwanted or suspicious calls, it also providers a "reverse look-up" function for users to input a number to identify the holder of that phone number, and to search for phone numbers using the name of an organisation or individual. The database of phone numbers and names was compiled from the phone books of the app users, which were allegedly collected by the operator of DU Caller without the consent of the holders of the phone numbers, or sometimes even without the knowledge or consent of the app users. Key government officials, such as the Secretary for Security of Hong Kong and the Privacy Commissioner, were included in the DU Caller database. This incident is reminiscent of the 3 mobile

9 See our article: "Do Not Disturb! Convictions for breach of the Direct Marketing Restrictions and Unsolicited Electronic Messages Ordinance": https://www.mayerbrown.com/files/Publication/98f5a31d-b5f1-4333-abb4-db11fefdf564/Presentation/PublicationAttachment/90274712-8db3-419a-a123-c128c4da060b/170323-ASI-IP-TMT-QuarterlyReview-2017Q1.pdf

Data Privacy Cont'd

apps that came to the attention of the PCPD in November 2016, which also involved a "reverse look-up" feature and the collection of users' contact lists[10]. Whilst the operators of the mobile apps and DU Caller app are not based in Hong Kong, and therefore do not fall within the jurisdiction of the PDPO, the individual app users residing in Hong Kong may still fall foul of the PDPO. Unsuspecting individuals would have provided their names and phone numbers to the relevant app user in order for them to store their details in their mobile device, for the purpose of enabling the app user to contact them. Such individuals are unlikely to have been aware of, or to have consented to, any transfer of their name and phone numbers to the app developers.

Takeaway Points

Personal data collected in a social context may be subject to the provisions of the PDPO. While the risk of complaints being filed by affected data subjects against an individual as a data user is low if the data user is an acquaintance, friend or member of one's family, the opportunity to use the privacy law as a bargaining chip in a family feud or dispute will not be lost on some. ◆

10 See our article: "Dodging your call: Collection of Contact Lists by Mobile Apps": https://www.mayerbrown.com/files/Publication/4e76421b-7c12-4d24-afe4-620ce0a41b34/Presentation/PublicationAttachment/7e947d52-0a47-4544-b2da-babaf665e476/161222-ASI-IP-TMT-QuarterlyReview-2016Q4.pdf

CHINA

Data Privacy

By Gabriela Kennedy, Partner, Mayer Brown JSM, Hong Kong
Xiaoyan Zhang, Counsel, Mayer Brown JSM, Shanghai

China Issues Interpretations on Criminal Offenses Involving Infringement of Citizens' Personal Information

On 9 May 2017, the Supreme People's Court and the Supreme People's Procuratorate of China issued rules that offer a clarification of the scope of criminal sanctions for breaches involving personal information in the form of Interpretations on Several Issues concerning the Application of Law in the Handling of Criminal Cases Involving Infringement of Citizens' Personal Information (**"Interpretations**"). The Interpretations shed light on the scope of the offence of "infringement of citizens' personal information" provided by Article 253 of the PRC Criminal Law. The Interpretations will come into force on 1 June 2017, the same date as the effective date of the PRC Cybersecurity Law (CSL) which was released on 7 November last year.

Specifically, Article 253 of the PRC Criminal Law (amended in 2015) imposes criminal sanctions on anyone who, in violation of relevant State rules, sells or discloses the personal information of third parties. The sanctions imposed by the statute vary depending on the seriousness of the circumstances of the violation. "Serious" circumstances attract prison sentences of no more than three years and/or a fine. "Extremely serious" circumstances see the penalties increased to three to seven years imprisonment, plus a fine. The sale or disclosure of personal information obtained in the course of conducting professional duties or providing services (such as postal services) attracts penalties at the harsher end of the spectrum.

The Interpretations provide much needed definitions to several key terms of Article 253. For example, "personal information" is defined to cover two types of information recorded through electronic or other means namely: i) any information that can be used alone or in combination with other information, to identify a natural person; and ii) any information reflecting the special characteristics of the activities of a natural person. The definition appears broader than the one provided by the CSL which was limited to the first category.

Data Privacy Cont'd

The Interpretations also clarify that "disclosure of personal information" punishable by Article 256 refers to acts of providing personal information to others without the consent of the data subjects. This term further covers acquisition of personal information through illegitimate means or during the course of performing duties and providing services. However, personal information that has been de-identified and cannot be traced back to an individual is excluded.

The criteria for the imposition of penalties is clarified in the Interpretations. For example, criminal detention or a fixed-term imprisonment of not more than three years, concurrently or separately with a fine, shall be imposed if one of the following "serious" circumstances applies:

a. Sale or provision of data pertaining to geographic location which is used by others to commit a crime;
b. Sale or provision of the personal information with actual or imputed knowledge that others would use the personal information to commit a crime;
c. Illegal procurement, sale or provision of more than 50 pieces of information concerning geographic location, content of correspondence, credit history, and financial assets of an individual;
d. Illegal procurement, sale or provision of more than 500 pieces of information concerning records of accommodation or correspondence, health, transaction, or other personal data that may affect the safety or any property/assets of an individual;
e. Illegal procurement, sale, or provision of more than 5,000 pieces of personal information concerning other information of an individual other than above;
f. The amount of information does not meet any of the requirements above, but the cumulative quantity of data alone meets the threshold imposed by the statute;
g. The illegal income derived from the provision of data exceeds RMB 5,000 (about US$722);
h. Sale or provision of personal information acquired in the course of conducting business or providing services, and the data involved exceeds half of the quota specified above;
i. The person committing the offence has been sentenced based on criminal or administrative charges for infringing provisions relating to personal information in the past two years; or
j. Any other circumstances.

Anyone who illegally purchases or obtains personal information in the course of their business shall be deemed to be violating Article 253 as well provided that the amount of illegal income exceeds RMB 50,000 (about US$7,221) or the person has been convicted of similar violations in the past two years.

The violations would be deemed "extremely serious" if the above acts lead to serious consequences such as death or significant economic losses, or when the amount of personal information involved exceeds more than 10 times the amount of any of the thresholds provided for "serious" circumstances. Extremely serious crimes shall attract sentences of a fixed-term imprisonment of three to seven years plus a fine.

Finally, Article 9 of the Interpretations imposes new obligations on network service providers. Any network service provider who fails to manage the security of information networks as provided by law and relevant administrative regulations and refuses to make corrections as ordered by regulatory authorities causing serious breaches of personal information shall be sentenced to criminal detention or fixed-term imprisonment of no more than three years, concurrently or separately sentenced to a fine pursuant to Article 286 of the PRC Criminal Law. Note that the CSL regulates network operators which are defined to include network service providers and, in addition, owners or administrators of networks.

The CSL has numerous enforcement provisions targeting operators of critical information infrastructures and network operators for violations of CSL specific obligations and duties such as the controversial data localisation governing "personal information" and "important data". The Interpretations serve as a strong companion to the CSL and address enforcement measures targeted specifically at breaches of obligations in relation to personal information, with arguably a clearer focus on the protection of citizens' privacy rights. ◆

HONG KONG

Cybersecurity

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

All "Hacked" Out: The Hong Kong Securities and Futures Commission Issues Proposals to Reduce Hacking Risks

On 8 May 2017, the Hong Kong Securities and Futures Commission (SFC) issued a consultation paper inviting comments on its latest proposals ("**Proposal**") aimed at reducing the risks of cyber attacks in relation to Internet trading. The consultation period ends on 7 July 2017.

Plugging the Hole

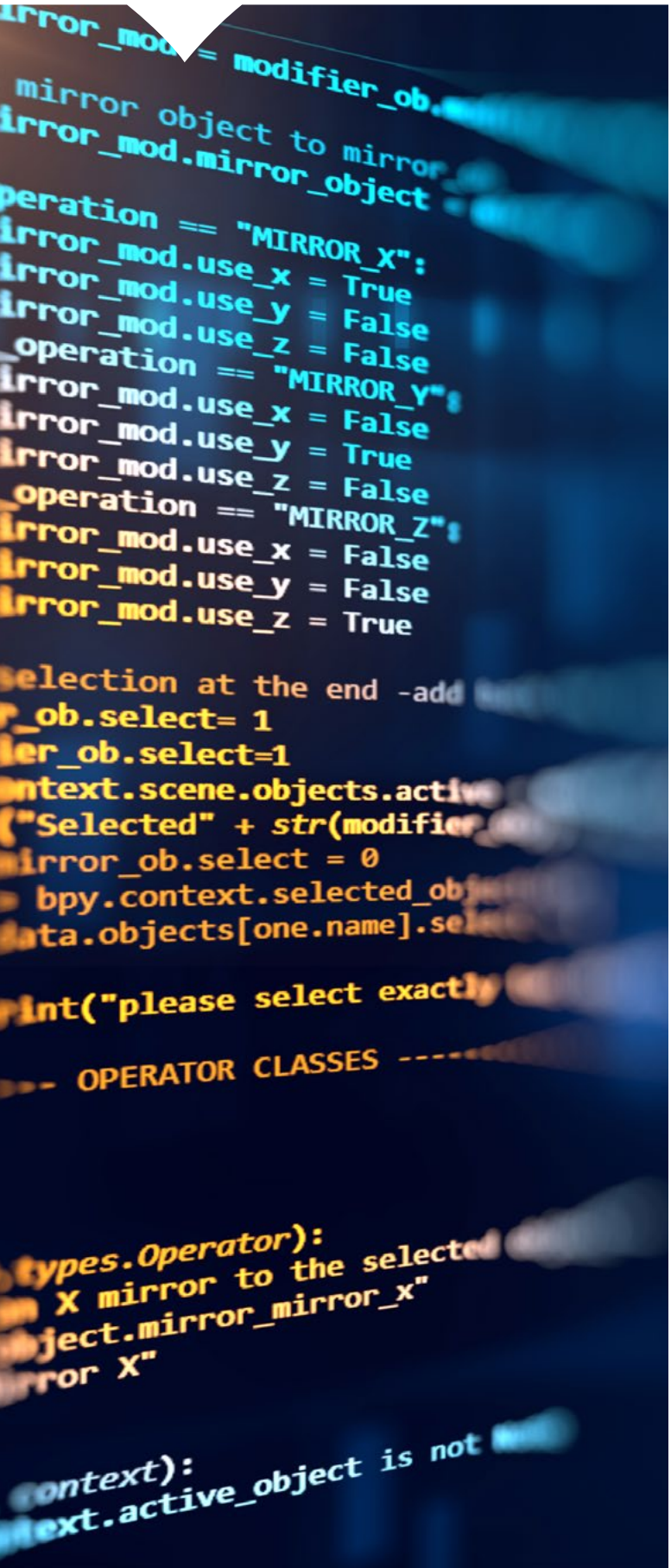
Since the beginning of 2016, at least 12 licensed corporations in Hong Kong have reported 27 cybersecurity incidents, which resulted in losses to investors worth HK$110 million. In January 2017, the police informed the SFC that several securities brokers had been victims of distributed denial of service (DDoS) attacks.

Over the past few years, the SFC has issued several circulars and recommendations to licensed corporations in an attempt to reduce the continuing surge of cyber attacks and to encourage the proactive implementation of robust cybersecurity measures. Licensed corporations are encouraged not to take a back seat and be reactive when it comes to their cybersecurity. Instead, they are asked to take responsibility at a managerial level and regularly review and test their systems, and address any risks identified.

In a recent circular issued on 26 January 2017, "Alert for Cybersecurity Threats", the SFC reminded licensed corporations that they need to implement appropriate safeguards without delay in order to protect themselves against cybersecurity threats. Licensed corporations were also reminded that any material cybersecurity incidents must be promptly reported to the SFC. Other related circulars include "Cybersecurity" dated 23 March 2016 and the "Tips on Protection of Online Trading Accounts" dated 29 January 2016.

The SFC is not the only regulator that is expending time and effort to tackle cyber attacks. The Hong Kong

Cybersecurity Cont'd



Monetary Authority (HKMA) launched the Cybersecurity Fortification Initiative on 24 May 2016[11], which introduced a cyber risk assessment framework, rolled out training to ensure a greater pool of qualified cybersecurity professionals, and set up a cyber intelligence platform for banks.

The Proposal is the latest in a stream of efforts by financial regulators in Hong Kong to tackle the increasing risk of cyber attacks. Following a review of the cybersecurity preparedness, compliance and resilience of brokers' Internet and mobile trading systems, conducted by the SFC at the end of 2016, the SFC identified several cybersecurity measures to help reduce the risk of cyber attacks. Whilst most of these measures have already been set out by the SFC in its Code of Conduct for Persons Licensed by or Registered with the SFC ("Code of Conduct") and in previous circulars, the SFC's intention is to consolidate them into a single guideline that provides further elaboration on existing recommendations. This culminated in the issuance of the Proposal and the launch of the consultation.

The Proposal

Under the Proposal, the SFC recommends the introduction of the draft Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading ("**Guidelines**"). The Guidelines are divided into three different categories of requirements, which cover: (i) the protection of clients' Internet trading accounts; (ii) infrastructure security management; and (iii) cybersecurity management and supervision.

The Guidelines do not introduce any surprising requirements – they are largely consistent with the existing requirements and recommendations of the SFC to date.

The key proposals of the SFC are as follows:

1. The SFC intends for the Guidelines to form baseline requirements that Internet brokers must comply

11 See our article entitled "Riding on the Crest of a Wave of Emerging Risks – New Initiatives on Cybersecurity by the Hong Kong Monetary Authority and the Securities and Futures Commission".

with, and will also form an entry requirement for future Internet brokers.

2. The SFC wishes to extend the scope of application of Paragraph 18 of Schedule 7 of the Code of Conduct to cover Internet trading of securities that are not listed or traded on an exchange. Currently, Paragraph 18 of Schedule 7 of the Code of Conduct only applies to securities dealers, futures dealers, leveraged foreign exchange traders and fund managers that conduct electronic trading of securities and futures contracts that are listed or traded on an exchange. However, some Internet brokers may conduct Internet trading through systems that are not listed or traded on an exchange, and would still be subject to the same hacking risks.
3. Under the Guidelines, the SFC intends to make two-factor authentication mandatory as a security measure for logging onto customers' Internet trading accounts. Two-factor authentication involves a combination of two different types of authentication measures (e.g., a combination of a password, a hardware or software token or biometric data), and is generally accepted as an effective means to reduce the risk of hacking. The Guidelines will not state exactly what type of two-factor authentication must be implemented, and brokers will have the flexibility to choose which method they deem appropriate.
4. The proposed baseline requirements will require brokers to use a secure network infrastructure through network segmentation, to monitor and assess security patches or hotfixes issued by service providers and implement them within one month, and to promptly update anti-virus and anti-malware solutions. Measures will also need to be implemented to prevent unauthorised installation of hardware and software and unauthorised access to the system and related servers or hardware (e.g., physical security controls). Only personnel who have a need to access the internal system should be granted such access rights, and remote access should be strictly limited on a need-to-have basis. Access lists will need to be reviewed on an annual basis to ensure that they are up-to-date.
5. The SFC recognised that encrypting the brokers' entire database would cause an adverse affect on the functioning of their Internet trading systems. As such, the SFC clarified that only customer login passwords stored on the brokers' systems will need to be encrypted, as well as sensitive information (e.g., trade data) during their transmission.
6. Under the Guidelines, brokers will need to have in place robust password policies for their customers, in order to minimise any unauthorised access. For example, minimum password lengths, a requirement that passwords be changed on a regular basis, etc. Session time out controls should also be implemented. During the activation of a customer's Internet trading account or any password resets, the password should be transmitted to the customer in a secure manner to avoid interception.
7. The SFC has decided not to make it mandatory for brokers to monitor suspicious trading patterns on their customers' Internet trading accounts, and will only suggest it as an example of good practice. Due to the large volume of data being transmitted, manual and automatic monitoring would be impractical. However, the SFC still expects brokers to have in place appropriate monitoring and surveillance mechanisms that will detect any unauthorised access to a customer's Internet trading account.
8. The SFC has included customer notification requirements in the draft Guidelines, as prompt notifications concerning activities on their Internet trading accounts (e.g., notifying them when someone has logged onto their account or when a transaction has been executed, etc.) can be an effective means of identifying and stopping hackers, since customers will be alerted to any unauthorised access or transaction. Due to the large volume of trade executions that a customer may carry out, the SFC proposes to allow customers to opt out of receiving trade execution notifications (but they cannot opt out of receiving

Cybersecurity Cont'd

other notifications, e.g., login or password changes).

9. The SFC has emphasised the need for brokers to implement a cybersecurity risk management framework, with the board or senior management having clear ownership and accountability for cybersecurity. Responsible and executive officers who are tasked with the overall management and supervision of the brokerage Internet trading system will be responsible for establishing the cybersecurity risk management framework, including the major roles and responsibilities, with the overall accountability resting with them.
10. The Guidelines will require brokers to implement written policies and procedures setting out how a cybersecurity incident should be reported and escalated (both internally and externally, e.g., to the SFC).
11. The Guidelines will require brokers to ensure their records and documents are backed up on an off-line medium on a daily basis, and to exercise reasonable efforts to ensure that their business continuity plan and crisis management procedures deal with different potential cybersecurity incidents. However, the SFC has decided not to make it mandatory for brokers to acquire DDoS solutions despite the recent spate of DDoS attacks, in light of the cost and the effectiveness of more affordable options.
12. Under the Guidelines, brokers will need to provide annual internal cybersecurity training, which should include recent cybersecurity regulations and threats. The SFC's 2016 review revealed that, despite staff playing a crucial role in minimising cyber attacks, many brokers had never provided internal cybersecurity awareness training or had only provided it irregularly on an ad hoc basis. The Guidelines also emphasise the need for brokers to take all reasonable steps to remind customers of potential cybersecurity risks and provide recommended measures to help customers protect themselves when using the Internet trading system.
13. It is common for Internet trading systems to be provided by third party service providers, rather than being internally developed and maintained by brokers. Consistent with previous circulars issued by the SFC, the Guidelines will require brokers that outsource any activities to a third party service provider to enter into a written agreement with them that sets out the terms of service and their responsibilities. These agreements should be regularly reviewed and amended, and should provide a sufficient level of maintenance and technical support, which can be quantitatively measured (e.g., specific service levels). It is important that the services and obligations of the service provider will ensure that the brokers will be compliant with the relevant regulatory requirements. However, under the Proposal, the SFC asks those in the industry to provide feedback on whether the current service levels provided by their service provider will enable them to comply with the Guidelines, and whether they anticipate any difficulty in obtaining a higher service level from their service providers (e.g., 99.9% service uptime).

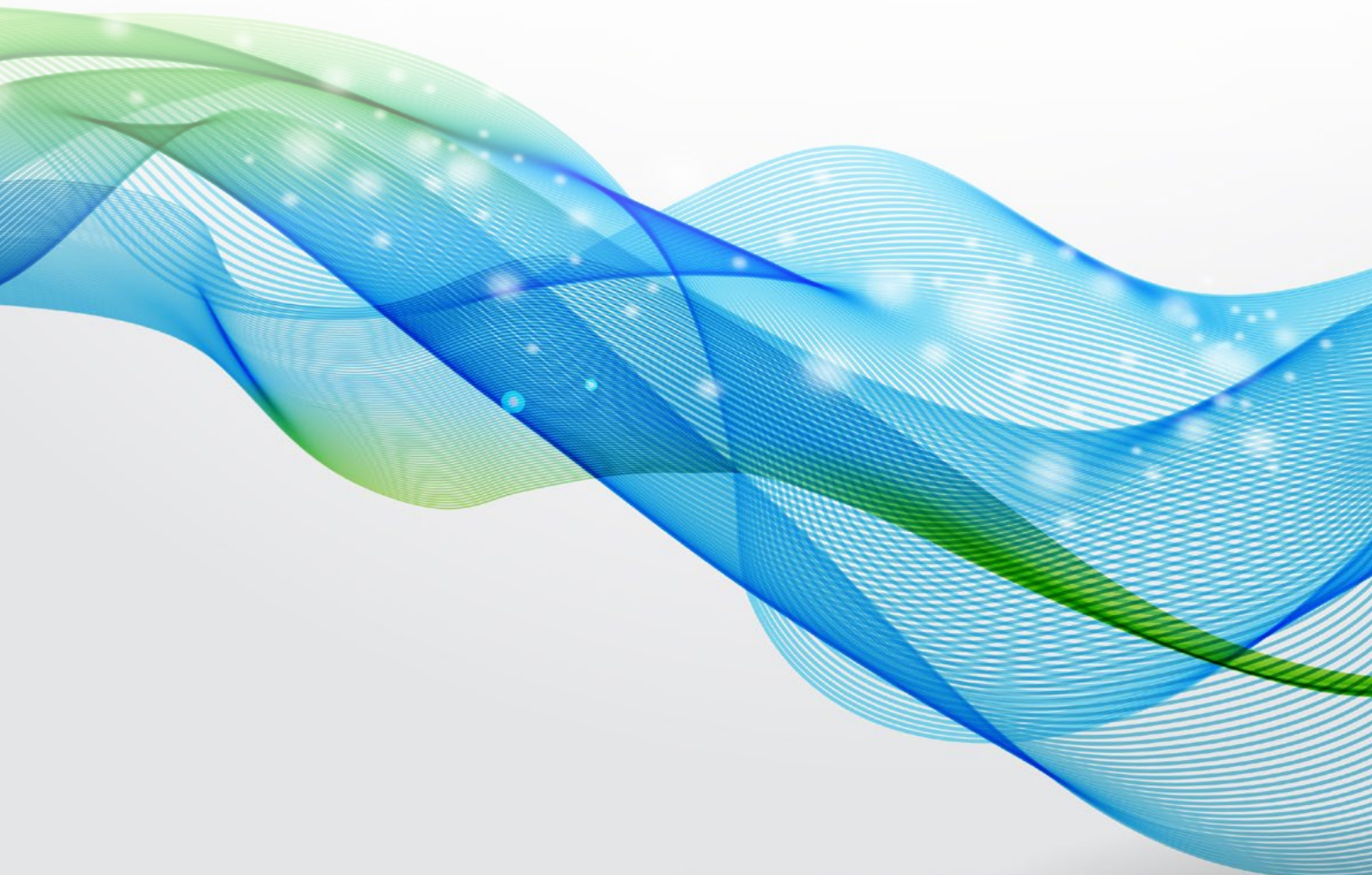
Conclusion

The review carried out by the SFC at the end of 2016 revealed that despite various cautions and guidelines in circulars issued by them so far on the subject of cybersecurity, brokers were still vulnerable to attacks. The main issues identified are: poor password policies; limited customer awareness of cybersecurity risks; inadequate monitoring and surveillance to detect unauthorised access or transactions; and insufficient resources deployed to boost cybersecurity. The draft Guidelines seek to introduce comprehensive and strict requirements and obligations on licensed corporations, the most important of which is clear ownership and accountability of cybersecurity management at the board or business management level.

Given the uptake in cloud and other outsourced services, brokers are advised to review such arrangements now in order to ensure that their service

providers are willing to work with them to meet the requirements set out in the Guidelines. Many service providers may operate on standard terms and conditions, and may be reluctant to tailor their methods of operation and security measures to meet the needs of individual clients. Regardless of the expediency of the procurement of popular services, given that accountability for cybersecurity management will rest with executive officers, all existing contractual arrangements for the provision of Internet trading systems will need to be revisited.

The SFC aims to finalise the revised Code of Conduct and new Guidelines by September/October 2017. Brokers will be given a grace period of six months from the date of publication of the final Guidelines in order to implement the baseline requirements. ◆



Contact Us

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

BENJAMIN CHOI
Partner
+852 2843 2555
benjamin.choi@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

VIVIAN OR
Senior Associate
+852 2843 2510
vivian.or@mayerbrownjsm.com

MAGGIE LEE
Associate
+852 2843 4336
maggie.lee@mayerbrownjsm.com

About Mayer Brown JSM

Mayer Brown JSM is part of Mayer Brown, a global legal services organisation, advising clients across the Americas, Asia, Europe and the Middle East. 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.