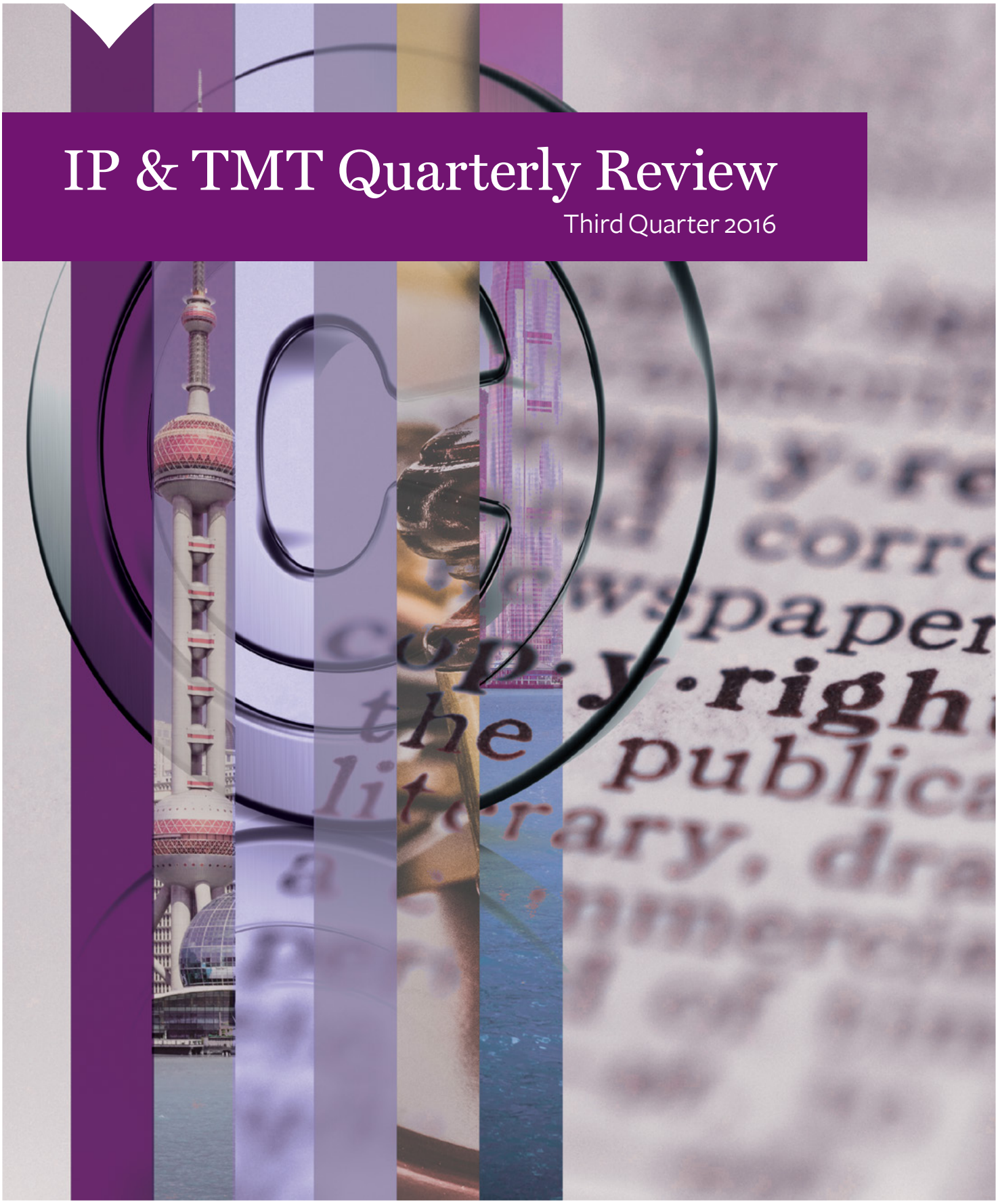
MAYER·BROWN
JSM

IP & TMT Quarterly Review

Third Quarter 2016



www.mayerbrownjsm.com

Content

Key: Click to Navigate

HONG KONG

Patents

By Xiaoyan Zhang, Counsel, Mayer Brown JSM, Shanghai
Maggie Lee, Associate, Mayer Brown JSM, Hong Kong

Delay No More: Amending Patents and the Lessons Learned in Celltrion, Inc v Genentech, Inc [2016] HKEC 1529

In July 2016, the Hong Kong Court of First Instance ("**CFI**") handed down a judgment allowing a patentee to amend its standard patent, which was facing a revocation action instituted by another company. In the judgement, the CFI set out the relevant factors to consider when determining whether or not to allow a patentee to make such amendments pursuant to Sections 102 and 103 of the Patents Ordinance (Cap. 514) (the "**Ordinance**").

Background – The Law on Amending Patents

According to Section 102(1) of the Ordinance, in any proceedings before a court in which the validity of a patent is at issue, the court may allow the patentee to amend the specification of the patent in such a manner, and subject to such terms as it sees fit regarding the related costs and expenses and the advertisement of the proposed amendment.

However, Section 103(3) of the Ordinance provides that any amendment of the specification of a patent pursuant to Section 102 will only be invalid to the extent that it extends the subject-matter disclosed in the application as filed or extends the protection conferred by the patent.

Facts of the Case

The defendant, Genentech, Inc ("**Genetech**"), was granted Hong Kong Standard Patent No. 1048260 entitled "Dosages for Treatment with Anti-ErbB2 Antibodies" (the "**Patent**") on 13 March 2009. The Patent was issued on the basis of a PRC patent (Chinese Patent No. ZL00814590.3) (the "**PRC Patent**") granted in 2008. The PRC Patent was subsequently declared invalid by the Patent Re-examination Board of the State Intellectual Property Office of the PRC.

In October 2013, the plaintiff, Celltrion, Inc ("**Celltrion**"), commenced revocation proceedings against Genentech to seek an order that the Patent be revoked on the grounds that it lacks novelty and an inventive step. Consequently, Genentech made two applications under Sections 102 and 103 of the Ordinance (the "**Applications**") to amend the Patent specification in July and August 2014, respectively.

By a consent order dated 2 February 2016, Celltrion was ordered, *inter alia*, to discontinue the revocation action upon its undertaking that it shall not oppose or otherwise contest the Applications. The Applications were therefore uncontested at the hearing.

The Court's Decision

The CFI accepted the Applications and allowed the proposed amendments to the Patent. The key questions that the judge considered were:

1. Whether or not the scope of proposed amendments fall foul of Section 103 of the Ordinance; and
2. Whether or not the Court should exercise its discretion under Section 102 of the Ordinance to allow the proposed amendments.

With respect to the first question, the judge was satisfied that the scope of proposed amendments would not fall foul of Section 103 of the Ordinance, as Genentech were simply seeking to limit the claims of the Patent under the first Application, and the second Application merely corrected a number of translation errors and typographical mistakes in the specifications.

Regarding the second question, the judge took into account the English and Australian case law relied on by Genentech and the Registrar of Patents. The CFI decided to follow the principles set out in the English case of *Smith, Line and French Laboratories Ltd v Evans Medical Ltd [1989] F.S.R. 561*, which state that:

a. The patentee bears the onus to establish that amendments should be allowed and it must make full disclosure of all relevant matters;
b. The amendments must be permissible under the Ordinance and no circumstances arise which would lead the court to refuse the amendment;
c. The amendment is sought promptly without unreasonable delay;
d. A patentee who seeks to obtain unfair advantage from a patent which he knows or should have known should be amended, will not be allowed to amend the patent (e.g., where the patentee threatens an infringer with his unamended patent after he knows or should have known of the need to amend it); and
e. The court is concerned with the conduct of the patentee and not with the merit of the invention.

In this case, Genentech had delayed in making the Applications. The Patent was granted in 2009 and the action was commenced in October 2013. However, the first Application was only made in July 2014. The CFI was not satisfied with the following explanation provided by Genentech for the delay:

a. Genentech had believed in the validity of the PRC Patent and thought its validity would be similarly upheld in Hong Kong;
b. In the absence of any marketing approval for the patented subject matter, Genentech had not found it necessary to consider enforcement action and did not reconsider the validity of the Patent in Hong Kong; and
c. No threat of enforcement action has ever been made in Hong Kong or elsewhere since the grant of the Patent.

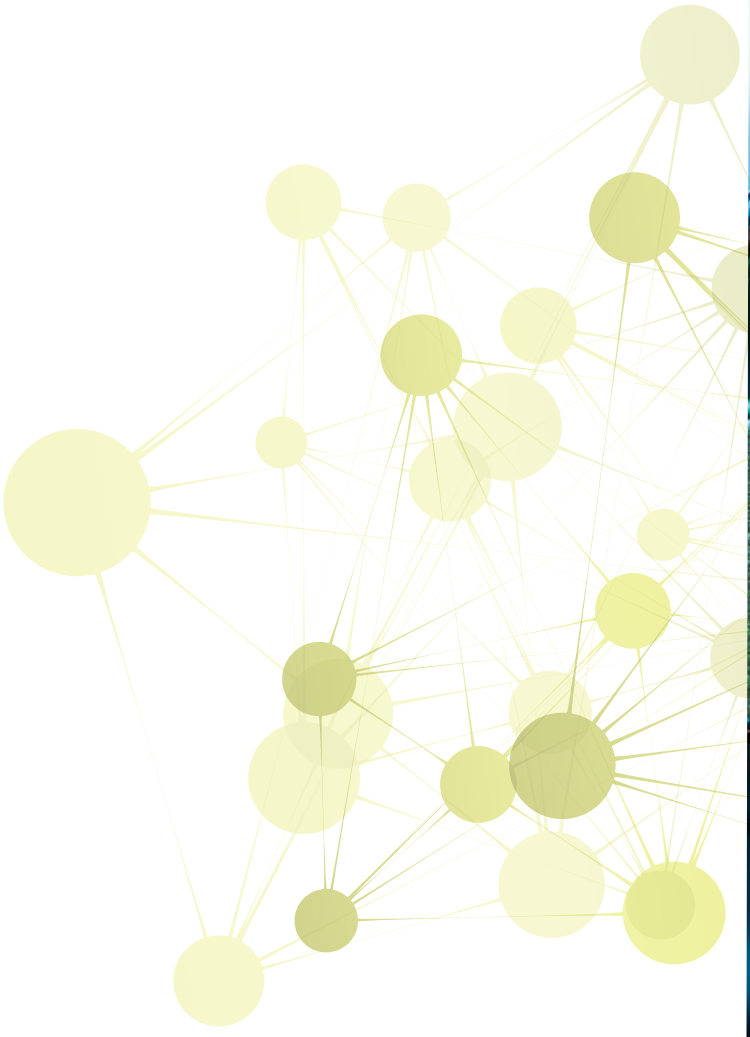
Nevertheless, the CFI was of the view that it had to take into account all of the circumstances of this case and could not simply focus on the issue of delay. In light of the fact that: (i) Genentech had not obtained any unfair advantage in its use of the Patent; (ii) there was no complaint of detriment arising from the delay; and (iii) neither Celltrion nor the Registrar of Patents opposed Genentech's amendments, the CFI decided to exercise its discretion to allow the proposed amendments to the Patent despite the delay.

Patents Cont'd

Conclusion

The CFI expects a patentee to apply for amendments to its patent as soon as reasonably practicable, although it will not merely focus on the issue of delay when considering whether or not to allow any amendments under Section 102 of the Ordinance.

Unsubstantiated belief in the validity of a patent or the fact that there has been no prior enforcement actions are unlikely to be considered an acceptable justification for a delay in the application, where the applied-for amendments are contested or there are complaints of detriment. ◆



Data Protection and Cybersecurity

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

Money for Nothing: Bitcoin Platform "BitFinex" Hacked in Hong Kong

On 2 August 2016, Hong Kong-based bitcoin exchange, Bitfinex, was hacked, resulting in 119,756 bitcoins worth approximately US$65 million being stolen. The exchange immediately halted trading and alerted its users of the security breach. This was the second-largest heist in a spate of hacks that have rocked the crypto-currency industry, the largest being Mt. Gox back in 2014, which ended up filing for bankruptcy after hackers stole about US$460 million in bitcoins.

Following the hack, Bitfinex has announced that it plans to issue tokens to its users equal to their losses, which may later be redeemed for shares in its parent company or exchanged for money. Bitfinex also stated that it intends to spread the loss equally amongst all of its users, including those that were not directly impacted by the hack. All users would stand to lose about 36% of their deposits.

What are Bitcoins? Are they Fungible?

Bitcoins are a peer-to-peer digital currency, which can be used to purchase goods or services. Bitcoins are fully decentralised and are not backed by any central bank or government, and therefore have no fixed exchange rate.

To avoid the risk of "double spending", the blockchain public ledger was created, which records every single transaction that occurs in the bitcoin economy. In addition to public blockchains, private blockchains are also available. As the name suggests, they are private networks that allow participants to update the ledger themselves. While blockchains successfully eradicate the "double-spending" problem, what about the fungibility of bitcoins as a crypto-currency? The blockchain allows bitcoins to be traced back to their origin, and thus stolen bitcoins can be tracked and rejected by merchants or trading platforms. This means that bitcoins are not necessarily interchangeable, and cannot be said to be fungible.

Data Protection and Cybersecurity Cont'd

In May 2014, the United States Internal Revenue Service confirmed that it would not treat bitcoins as a currency, but that it would view them as property or stock. Similarly, in Hong Kong, the regulatory authorities have consistently stated that bitcoins are a virtual commodity, rather than a virtual currency. It is therefore likely that bitcoins will not be treated as fungible in Hong Kong either. This will impact the remedies available to individuals whose bitcoins are stolen.

The Hong Kong Financial Secretary announced in his latest 2016-2017 Budget Speech, that the Hong Kong Government intends to encourage organisations to explore the potential application of blockchain technology for financial services, with the aim of reducing anti-money laundering or other shady transactions, and to reduce costs[1]. It is likely therefore that we may see more interest in private blockchains in Hong Kong in the future.

Recovering Losses

Bitcoins are not specifically regulated under Hong Kong law nor are they subject to the supervision of the Hong Kong Monetary Authority or the Securities and Futures Commission. However, the general laws concerning anti-money laundering, anti-terrorist funding, fraud, theft and computer crimes may still apply in relation to certain bitcoin activities. For example, the person who hacked into Bitfinex's system and stole the bitcoins may be guilty of an offence in Hong Kong on the basis that they gained unauthorised access to a computer with a view to dishonest gain or to cause loss to another (Section 161 of the Crimes Ordinance (Cap. 200)).

Users who suffered a loss as a result of the hack may seek civil remedies. This has not yet been tested in the Hong Kong courts, and there is uncertainty as to the level of liability of bitcoin trading platforms. Users may try to argue that the trading platform owed them a duty of care and acted negligently by failing to have in place sufficient security measures to prevent the cyber-attack from taking place. Alternatively, users could try to bring an action on the basis of breach of contract. Whether or not such negligence or breach of contract claims could be successful will depend significantly on the circumstances of each case.

In the event of liquidation of the bitcoin trading platform, would the customers have a claim against the trading platform and could they be entitled to the platform's assets as creditors? In the Mt. Gox case (where about US$460 millions worth of bitcoins was stolen in 2014), during the liquidation proceedings, the company was found liable for all losses suffered by its customers, as the funds received from its customers were co-mingled into a single pool and so ownership and title to the actual bitcoins was deemed to be held by Mt. Gox (not the customers). Mt. Gox therefore owed its customers an amount equivalent to the bitcoins, and not the bitcoins themselves, meaning that its customers were entitled to part of Mt. Gox's assets as a creditor.

In contrast, Bitfinex segregated the amounts it received from its customers and held them separately. In such circumstances, ownership and title to the bitcoins appear to remain with Bitfinex's customers, with Bitfinex merely acting as a custodian. Customers of Bitfinex may not be regarded as creditors and therefore they may not be able to make a claim against Bitfinex's assets. They may only be entitled to their actual bitcoins still held by Bitfinex in the relevant customer's account (if any).

With regard to the stolen bitcoins, the blockchain system may allow victims to trace their bitcoins to find out the identity of the recipient. As bitcoins are generally viewed as non-fungible property (rather than as a currency or cash), victims of hacks may be able to recover their stolen bitcoins from the ultimate recipient.

1 http://www.legco.gov.hk/research-publications/english/essentials-1516ise15-blockchain-technology.htm

Conclusion

Despite the latest stream of hacking incidents, the use of bitcoins is gaining popularity. In most countries, including Hong Kong, bitcoins and bitcoin trading platforms are largely unregulated, with little or no protection expressly provided to users under the law. In the event of fraud on a bitcoin trading platform and/or hacking incidents, bitcoin users may be left with little recourse against the trading platforms.

The continued growth of bitcoins cannot be ignored, and it is likely that before too long the bitcoin market will begin to be regulated. For example, in May 2016, Japan passed an amendment to its current financial laws requiring the regulation of virtual currency exchanges by the Japan Financial Services Agency. The amendments will come into force within a year after its official publication, and will require all crypto-currency exchanges to be registered and subject to the supervision of the Financial Services Agency. Japan is one of the first jurisdictions in Asia to expressly impose bitcoin regulations. Bitcoin trading in Japan has spiked this year, which may be tied to the passing of the virtual currency legislation.

Regulation of the bitcoin market will help to further encourage the uptake of bitcoins by individuals and service providers, with protections in the bitcoin market becoming enshrined in legislation. Until such time, *caveat emptor*! ◆

Data Protection and Cybersecurity

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

Bring Home the Data? New Hong Kong Data Privacy Guidelines for BYOD Policies

On 31 August 2016, the Hong Kong Privacy Commissioner ("**PC**") issued a new Information Leaflet to highlight the personal data privacy risks that employers need to address when developing a Bring-Your-Own-Device ("**BYOD**") practice ("**Information Leaflet**"). This new Information Leaflet has been issued against the backdrop of increasing cybersecurity concerns, particularly in the financial industry.

Cybersecurity Risks

BYOD practices are not new. They are now almost common place, to the point where they are now taken for granted. It is at such times that risks are overlooked in the rush to "be like everyone else" and have a BYOD practice in place. BYOD practices introduce new vulnerabilities to a company's cybersecurity. As BYOD policies allow employees to use their own personal devices (e.g., tablets, laptops, smartphones, etc) for employment related activities, companies have less control on how their employees access and use personal data belonging to the company (e.g., customer data). Unlike organisation-owned devices, personal devices are generally more vulnerable to cyber attacks or to accidental data leakages.

It is no surprise that the financial industry, which has been the most active with regard to cybersecurity, has also taken the lead in relation to BYOD practices, due to the sensitive nature of personal data handled by banks and the significant consequences that may be suffered if data is stolen, lost or misused. Since at least 2014, the Hong Kong Monetary Authority ("**HKMA**") and the Securities and Futures Commission ("**SFC**") have been actively requiring financial institutions to step up their risk management and cybersecurity measures. In October 2014, the HKMA issued a revised Circular on Customer Data Protection, which removed restrictions

on BYOD policies for financial institutions, but required them to comply with the Recommended Standards of Bring Your Own Devices for Work by Bank Staff in Hong Kong issued by the Hong Kong Association of Banks. In parallel, on 6 October 2014, the PC also issued a Guidance Note on the Proper Handling of Customers' Personal Data for the Banking Industry[2].

One of the more recent developments in the financial industry, was HKMA's announcement on 18 May 2016 of the launch of a new cybersecurity fortification initiative ("**CFI**"). The CFI aims to enhance the cybersecurity of Hong Kong's financial industry through[3]:

a. The introduction of a cyber risk assessment framework;
b. Making appropriate training available to ensure a steady supply of qualified cyber security professionals; and
c. Setting up a cyber intelligence platform for financial institutions to share information to enhance collaboration.

Protecting Personal Data

On 31 August 2016, the PC issued the Information Leaflet to try and help companies continue to comply with the Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**")[4], as BYOD practices are becoming increasingly widespread across all industries.

Although companies may already have in place general policies on data protection with which their employees are required to comply, BYOD practices present their own risks and introduce new concerns which need to be specifically addressed through individual policies. Companies need to protect both personal data accessed and used by its employees on their devices (e.g., customer data), and also employees' personal data transmitted from their device back to their employer.

RETENTION OF PERSONAL DATA

Companies must assess whether or not to allow their employees to save personal data on their personal devices, and how their internal retention and erasure policies need to be amended to deal with such situations. Under the PDPO, data users must take all practical steps to ensure that personal data held by them is not retained for longer than necessary in order to fulfil the original purpose (or a directly related purpose) of collection. A company may be in breach of the PDPO if their employees continue to maintain customers' personal data on their device, beyond the relevant retention period.

In practice, it will be difficult for an employer to be certain that all business related information is no longer retained by a former employee (e.g., stored on their personal devices). Whilst employer's internal policies may make it a requirement that employees erase or return all work-related data stored on their personal devices, verifying and enforcing this in practice may be more difficult.

We would recommend that companies:

a. Prohibit and implement technical measures to prevent employees from saving any work-related data (including personal data) on their personal device, and requiring all documents and data to be saved on the company's secure system, which can be remotely accessed by the employee via their device;
b. Alternatively, implement technical measures that enable the company to remotely delete all company data stored on the employee-owned device, without affecting any of the employees' other

2 For further details, please refer to our article "*Banking On Your Personal Data: Recent Guidance Issued to Banks*": https://www.mayerbrown.com/files/Publication/7697fa24-69e7-4839-9c5e-7f4e7464004a/Presentation/PublicationAttachment/54705832-9382-44e4-9022-8c1b6592e829/141223-HKG-BF-FSRE.pdf

3 For further details on the CFI, please refer to our article "*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*": https://www.mayerbrown.com/files/Publication/b9b1ed67-cbef-46f0-901c-2a05391ab000/Presentation/PublicationAttachment/5a502076-501e-488b-bc93-09bf6df6c922/160630-ASI-IP-TMT-QuarterlyReview-2016Q2.pdf

4 https://www.pcpd.org.hk//english/resources_centre/publications/files/BYOD_e.pdf

Data Protection and Cybersecurity Cont'd

personal data or documents (this will require any company data to be segregated and stored in one area of the device); and

c. Requiring employees to sign an undertaking to delete all data stored on their personal device once it is no longer needed for the relevant work-related purpose and once their employment comes to an end.

TRANSFER AND USE OF PERSONAL DATA

Companies must establish controls on how personal data collected by them can be accessed, used and transferred by their employees – both on company-owned equipment and on employees' personal devices. Companies should implement policies and send regular reminders to prevent their employees from using such data in breach of the PDPO, by clearly stating how the data can be used, to whom it can be transferred, etc.

SECURITY MEASURES

Personal devices are inevitably less secure then company-owned equipment. Companies generally spend time and money on implementing robust systems and safeguarding measures to prevent cyber attacks and misuse of data. In comparison, personal smartphones or tablets are relatively vulnerable to attacks or viruses. Companies must ensure that their employees' personal devices have in place additional safeguards to protect them.

However, the implementation of security measures on an employee's device must be balanced against the employee's own right to privacy, and the usual measures that a company might employ in respect of company-owned devices may not be appropriate for employee-owned equipment. For example, implementing tracking software on an employee-owned device or having the ability to remotely access the device are unlikely to be appropriate and may infringe the employee's data privacy rights. Therefore, some of the safeguarding measures proposed by the PC include less intrusive methods, e.g., preventing company-owned data from being stored locally on the employee's devices, using dedicated usernames, passwords and screen locks, and encrypting the personal data stored on the device, which must be commensurate to the sensitivity of the data. Another alternative would be to implement technical solutions to segregate company-owned data from other information in the employee-owned device, which can then be wiped remotely without affecting any other data of the employee.

DATA ACCESS AND CORRECTION REQUESTS

A company's obligation to comply with data access and data correction requests of data subjects under the PDPO, applies equally to any personal data of such data subjects that are stored by the company's employees on their personal devices. Therefore, companies must have an internal procedure in place to enable them to comply with such requests, e.g., making sure that all company-owned data is backed up on a system controlled by the company, and not only saved on an employee's device.

Best Practices

Under the Information Leaflet, the PC recommends that companies establish a BYOD policy, conduct a risk assessment and apply technical solutions to protect personal data. Companies must also carry out regular reviews to assess compliance with their current internal policies and check for new threats and vulnerabilities, and update their policies and measures accordingly.

Before implementing a BYOD policy, companies should carry out a risk assessment to determine the types of personal data that can be accessed or stored on an employee's device, and the potential harm and likelihood of unauthorised loss or disclosure. The risk assessment should also take into account the privacy implications on the amount of personal data of the employee (or their friends and family), which can be accessed on their device. Based on the results of its risk assessment, a company should then develop its BYOD policy and determine what technical solutions be implemented.

The BYOD policy must set out the specific roles and responsibilities of the company and its employees, and the criteria by which a company determines what can be accessed via the employee-owned device and the type of device allowed. The BYOD policy must also specify the technical methods utilised to protect the personal data owned by the company and its employees' personal data, and how the company monitors compliance with the policy and what are the consequences for non-compliance.

The technical solutions implemented by a company to protect company-owned data, must be balanced against the employees' right to privacy. Some of the PC's recommended security measures include implementing an independent and additional password protection and access control, on top of the employee-owned device's current security setting (i.e. requiring complex passwords and double authentication, and automatic time-out following inactivity, etc); additional encryption of company-owned personal data stored on, or transmitted to and from, the employee-owned device; and automatic deletion of sensitive company-owned personal data stored on the employee-owned device in certain circumstances (e.g., repeated input of incorrect passwords, etc).

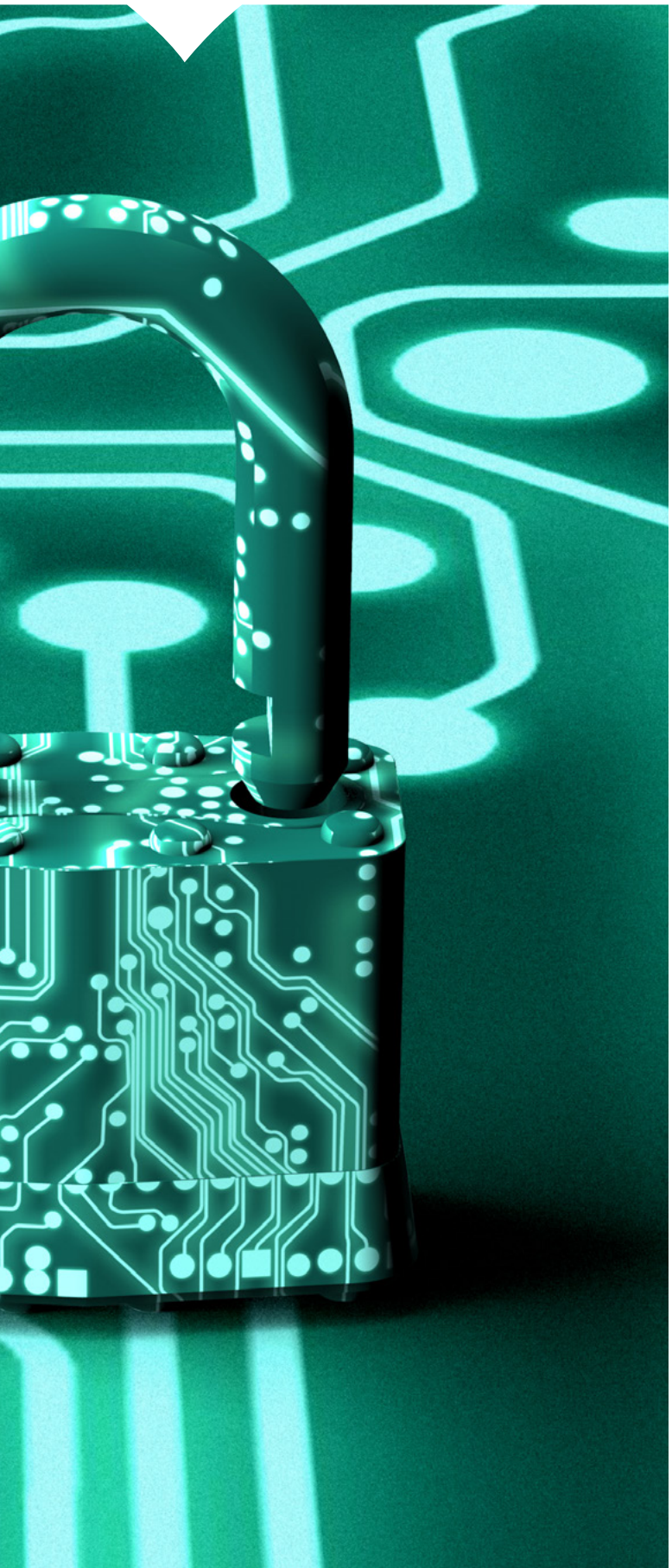
Conclusion

Does the adoption of a BYOD practice bring benefits that outweigh the data privacy and cybersecurity risks it introduces? Do your internal policies and practices sufficiently take into account and minimise the risks presented by your BYOD practice? Do your internal policies sufficiently protect the employees' right to privacy in respect of their personal devices?

A balance needs to be struck between protecting the personal data collected by a company and respecting the privacy of their employees' own personal data. Whilst security measures need to be robust, they cannot be so intrusive as to infringe the employees' own right to privacy or result in a potential unfair or excessive collection of employees' personal data stored on their device. A detailed risk assessment should be carried out, and a BYOD policy implemented to address the specific concerns presented by BYODs. Such assessments and internal policies cannot be static. In light of the fast-paced changes in technology, companies must carry out regular reviews of their internal policies and security measures to stave off any vulnerabilities that could result in cyber attacks or accidental loss or disclosure by employees. ◆

Data Protection and Cybersecurity

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



More Money, More Worries?

Stored Value Facility Licensing Requirements and Privacy Concerns

On 25 August 2016, the HKMA announced that it had granted five stored value facility ("**SVF**") licences[5], which are the first set of such licences granted by the Hong Kong Monetary Authority ("**HKMA**") under the new Payment Systems and Stored Value Facilities Ordinance (Cap. 584) ("**PSSVFO**"). On the same date, the Hong Kong Privacy Commissioner ("**PC**") issued a statement setting out advice on the collection of personal data by operators of SVFs in light of the sensitive data that may be involved.

Stored Value Facilities and Retail Payment Systems

On 13 November 2015, the new regulatory regime for SVFs and retail payment systems ("**RPS**") came into operation under the PSSVFO (formerly the Clearing and Settlements System Ordinance). Under the PSSVFO:

a. Issuers of both device and non-device based multi-purpose SVFs must obtain a licence from the HKMA (note that licensed banks will already be deemed to have the necessary licence to carry on an SVF business, and single-purpose SVFs are not subject to the licensing requirements)[6]; and

b. The HKMA has the power to designate RPSs that will be subject to its oversight[7].

5 http://www.hkma.gov.hk/eng/key-information/press-releases/2016/20160825-3.shtml

6 See the HKMA's Explanatory Note on Licensing for Stored Value Facilities issued in November 2015: http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/infrastructure/retail-payment-initiatives/Explanatory_note_on_licensing_for_SVF.pdf

7 See the HKMA's Explanatory Note on Licensing for Stored Value Facilities issued in November 2015: http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/infrastructure/retail-payment-initiatives/Explanatory_note_on_licensing_for_SVF.pdf

For further details on the PSSVFO, please see our previous articles "*Aligning the law with innovative payments in Hong Kong*"[8] and "*Hong Kong's proposed new payments regulatory regime*"[9] published in the E-Finance & Payments Law & Policy in October 2013 and November 2014 respectively, and "*Out With the Old, and In With the New: Amendments to the Payment Regulations in Hong Kong*"[10].

The provisions concerning the application and processing of SVF licences and the designation of RPSs came into operation on 13 November 2015. SVF operators were provided with a twelve month grace period to obtain the required SVF licence. The grace period comes to an end on 13 November 2016. From 13 November 2016 onwards, it will be an offence to operate a multi-purpose SVF without a licence in Hong Kong.

Personal Data Protection

On 25 August 2016, the PC issued a statement offering advice on the protection of personal data in the context of SVFs[11]. SVF operators must consider the level of personal data they need to collect from customers – such collection should be no more than is necessary in order to provide their services. The more personal data an operator collects, the greater the risk of being in breach of the Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**") or being vulnerable in the event of a cyber attack.

SVF operators are reminded to fully comply with the requirements under the PDPO (e.g., their notification requirements, direct marketing restrictions, security requirements and obligation to comply with data access and data correction requests, etc). In addition, the PC also recommends the following:

a. Privacy should be the default starting position of SVFs, and users should be given the option to decide what personal data can be accessed or collected by the SVF operator. Users should be allowed to withdraw their consent at any time, without prejudicing their right to use the SVF, to the extent possible. This obligation to minimise the amount of personal data collected is of course subject to the licensees anti-money laundering obligations under the PSSVFO.

b. SVF operators are advised to be transparent about the personal data they collect, how the data will be used and to whom it will be transferred. Such information must be presented to customers in compliance with the PDPO, and in a simple, user-friendly manner.

c. If an SVF operator intends to use the personal data of a customer for any purpose not directly related to the payment service, then it should obtain the explicit consent from the relevant customers. This recommendation goes beyond simply obtaining the customers' express consent for use of their personal data in direct marketing, and could apply to any purpose outside of the payment service.

d. SVF operators should carry out formal risk assessments on a regular basis to ensure that the level of security used to safeguard the personal data held by it are commensurate with the types of data held, i.e. the more sensitive the personal data, then the greater the security measures.

e. SVF operators that engage third party agents to process personal data on their behalf, must utilise either contractual or other means to ensure that the personal data transferred to the third party agent are not kept longer than necessary, and safeguarding measures are implemented by the third party agent to prevent unauthorised or accidental access, processing, erasure, loss or use of the data.

8 http://www.mayerbrown.com/files/News/e8cbc456-f7ba-493b-a008-09de3e7b7c64/Presentation/NewsAttachment/45a24d44-8391-4052-996a-0be600c70801/Aligning%20the%20law%20with%20innovative%20payments%20in%20Hong%20Kong.PDF

9 http://www.mayerbrown.com/files/News/dc594ac3-8938-42b9-9d12-2c48c5fa4eba/Presentation/NewsAttachment/68fce6e6-687b-4ad7-8a7a-2c8e8c07dcf0/EFPLP%20November%202014%20pg%2013-14.pdf

10 https://www.mayerbrown.com/files/Publication/6947e0fb-496c-4744-90a2-74401e79bed7/Presentation/PublicationAttachment/387c6e22-b40e-4d03-bc31-af8a233d74ed/IP%20%26%20TMT%20Quarterly%20Review_2015%20Q1.pdf

11 https://www.pcpd.org.hk/english/news_events/media_statements/press_20160825.html

Data Protection and Cybersecurity Cont'd

Conclusion

Time is running out, and the expiry of the grace period for operating a multi-purpose SVF without a licence is fast approaching. Multi-purpose SVF operators must commence the process of obtaining an SVF licence as soon as possible. If a licence is not issued by 13 November 2016, then the relevant SVF business will need to consider their contingency plans. The continued operation of a multi-purpose SVF business after 13 November 2016, without a licence, could give rise to a maximum fine of HK$1,000,000 and 5 years imprisonment upon conviction on indictment.

SVF operators should also carry out a privacy due diligence exercise to ensure that their internal procedures are in-line with the PDPO and their security measures are sufficient. Major headlines regarding PC investigations, customer complaints or cyber attacks could not only cause irreparable damage to the relevant company's reputation, but could also weaken public confidence in mobile payments and e-wallets, and hinder the general public uptake of new payment methods. ◆

CHINA

Cybersecurity

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

China Releases Guidelines to Strengthen Cybersecurity Standardisation

On 12 August 2016, the Cyberspace Administration of China ("**CAC**"), the General Administration of Quality Supervision, the Inspection and Quarantine of China ("**GAQSIQ**"), and the Standardisation Administration of China ("**SAC**") jointly released *Several Guidelines to Strengthen National Cybersecurity Standardisation* (the "**Guidelines**"). Under the Guidelines, mandatory national standards will be introduced to regulate critical fields such as major information technology infrastructure and classified networks in an effort to harmonise the current divergent local practice.

The National Information Security Standardisation Technical Committee will be the agency solely responsible for the review, approval, and release of national cybersecurity standards. The Guidelines propose to enhance the role of cybersecurity standards in guiding industrial development by, *inter alia*, establishing a standard-sharing mechanism for major cybersecurity projects as well as by incorporating standard requirements into the evaluation criteria of such projects and setting up professional qualifications. The Guidelines also stress the importance of establishing essential standards such as the "Internet +" Action Plans, "Made in China 2025," and "Action Plans for Big Data" for critical projects such as big data security and cybersecurity audits. Finally, the Guidelines call for China's active participation in international standard-setting activities with the aim of elevating China's influence at the international level. As a sign of commitment to this, China will selectively adopt international standards which are deemed to suit China's own situation.

The release of the Guidelines, on the one hand, is consistent with the Chinese government's intent to have a tighter grip over China's Internet and

CHINA

Cybersecurity Cont'd

networks. On the other hand, standards unification will likely improve the transparency of cybersecurity governance and the predictability of cybersecurity enforcement, a positive step as we are still waiting for the finalisation of the draft Cybersecurity Law. While the content of the national cybersecurity standards may be redolent of heavy "Chinese characteristics," there is a glimmer of hope as China has now signalled a desire to be involved in international cybersecurity standards-setting. ◆

HONG KONG

Telecommunications

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

Broadcasting Ordinance: When does the Internet Exception Apply?

In a recent case, *Secretary for Justice v Hong Kong Cable Television Limited [2016] HKEC 1163*, the domestic pay-television service provider, Hong Kong Cable Television Limited ("**i-Cable**") was ordered by the Court of Appeal to pay the Communications Authority ("**CA**") a prescribed fee as a licensee for domestic pay-television services. The main points of contention were the formula to calculate the licence fee and whether the 'Internet Exception' under the Broadcasting Ordinance (Cap. 562)[12], applied to i-Cable's domestic pay-television service ("**Service**").

Background

The Service was provided digitally through the Internet. The infrastructure, specifically the set-top boxes, through which the domestic pay-television programmes ("**Television Programmes**") were transmitted, were installed in the common areas of residential buildings. The set-top boxes decoded the Internet packets transmitted from i-Cable into analogue audio-visual signals for transmission to individual flats by way of a cable known as the 'In-Building Coaxial Cable Distribution System' in order for residents to view the Television Programmes.

Under the Broadcasting Ordinance, a service provider which provides services outside of the 'Internet Exception' (i.e. any service provided via the Internet) has to pay the CA a prescribed licence fee. The CA argued that i-Cable's Service fell outside the 'Internet Exception', and claimed the prescribed licence fee for the years 2007, 2008 and 2009 from i-Cable, to be calculated on the basis of the number of individual flats which received the Service.

However, i-Cable contended that the Service did fall within the 'Internet Exception', and even if this was not

12 Under section 5 of Schedule 3 of the Broadcasting Ordinance.

Telecommunications Cont'd

the case, that the prescribed licence fee should be calculated on the basis of the number of buildings or estates which received the Service.

Court of First Instance

The Court of First Instance held that i-Cable's Service did fall within the 'Internet Exception'. However, as this exception required i-Cable to transmit programmes using a globally unique IP address[13] and since i-Cable only started using this in 2008, it needed to pay variable licence fees for 2007 and 2008. The judge agreed with the CA that the fee should be calculated on the basis of individual flats.

Court of Appeal

The Court of Appeal reversed the Court of First Instance's decision and held that i-Cable's Service fell outside of the 'Internet Exception', and that the licence fee should be calculated based on the number of individual flats which had received the Service.

Court of Appeal Rationale

Interestingly, the determining factor as to whether the Service fell within the 'Internet Exception' was the location of the set-top boxes. In this case, the set-top boxes decoded the Internet packets transmitted from i-Cable into analogue audio-visual signals for transmission to the individual flats of the residential buildings by way of cable, which meant that the Internet packets "stopped" at the set-top boxes.

The Court of Appeal held that Television Programmes require an audience "*to enjoy and to view*" the programmes. It went on further to state that this audience has to be the residents in the individual flats of the buildings. The Court of Appeal did not agree that the programmes were transmitted by way of Internet exclusively, as it deemed there was no audience enjoying or viewing the Television Programmes in the common areas of the buildings where the set-top boxes were installed. The Television Programmes were therefore transmitted to the residents by cable rather than the Internet.

As for the calculation of the licence fee, although i-Cable entered into subscription agreements with the management companies of the buildings, the 'subscribers' were held to be persons with the 'right to view' the programmes - in this case the residents of the individual flats.

Conclusion

With this decision, the Court of Appeal has clarified the position for broadcasting licensees aiming to assert that their services fall within the 'Internet Exception'. ◆

13 A 'globally unique IP address' is an address that is dedicated exclusively to a single hosting account. The IP address is not shared with other websites and allows access to the website just by keying in the unique IP address alone. Its function is essentially the same as a postal address; only it is used on the Internet.

Contact Us

GABRIELA KENNEDY
Partner
+852 2843 2380
gabriela.kennedy@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

AMITA HAYLOCK
Senior Associate
+852 2843 2579
amita.haylock@mayerbrownjsm.com

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