

MAYER • BROWN
JSM

IP & TMT Quarterly Review

Table of Contents

2	TRADE MARKS – HONG KONG Hong Kong Issued Consultation Paper on Joining the Madrid Protocol
4	TECHNOLOGY – CHINA MIIT Issued Draft SMS Rules for Consultation
6	DATA PRIVACY – HONG KONG Banking On Your Personal Data: Recent Guidance Issued to Banks
12	DATA PRIVACY – HONG KONG To Search or Not to Search? Does the Right to Privacy Prevent the Police from Seizing and Searching Mobile Phones in Hong Kong?
16	TECHNOLOGY – HONG KONG The Future of Innovative Payments
21	CONSUMER PROTECTION – HONG KONG Recent changes to the Toys and Children’s Products Safety Ordinance
23	CONTACT US



Hong Kong Issued Consultation Paper on Joining the Madrid Protocol

By Rosita Li, Partner, Mayer Brown JSM, Hong Kong

Benjamin Choi, Partner, Mayer Brown JSM, Hong Kong

On 11 November 2014, the Commerce and Economic Development Bureau and the Intellectual Property Department of the Hong Kong Government jointly issued a consultation paper on the proposed application of the Protocol Relating to the Madrid Agreement Concerning the International Registration of Marks (“Madrid Protocol”) to Hong Kong. The three-month consultation will end on 11 February 2015. The purpose of this consultation is to gather views on the benefits, implications and implementation of the application of the Madrid Protocol to Hong Kong.

FEATURES OF THE MADRID SYSTEM

The Madrid System for international registration of trade marks is administered by the World Intellectual Property Organization and governed by the Madrid Agreement Concerning the International Registration of Marks (“Madrid Agreement”) and the Protocol Relating to the Madrid Agreement Concerning the International Registration of Marks (“Madrid Protocol”).

With the introduction of the Madrid Protocol to Hong Kong, applicants domiciled or registered in Hong Kong (whether individuals or businesses) will be able to file applications to register their trade marks in multiple Madrid Protocol member countries by way of a single filing and registration process without the need to file separate applications with different local trade mark offices. Foreign companies holding existing International Registrations of trade marks will also have the option to expand the territorial protection of their marks by designating Hong Kong without the need to file a separate domestic application in Hong Kong.

CURRENT TRADE MARK ENVIRONMENT IN HONG KONG

At the moment, foreign companies have to file separate applications in Hong Kong in order to protect their trade marks here. Similarly, Hong Kong companies will need to file separate applications in those other jurisdictions to which they wish to extend their trade mark protection.

Statistics show a steady increase in the number of trade mark applications filed with the Hong Kong Trade Marks Registry in recent years, with a noticeable jump of 50% within 4 years (2009 to 2013) in both the total number of applications and the number of applications filed by overseas applicants.

More than 30% of the overseas filings came from applicants in the People’s Republic of China (“PRC”). These figures show that Hong Kong has become an increasingly popular jurisdiction for trade mark protection for overseas trade mark owners.

At the same time, there has also been a 50% increase from 2008 to 2013 in the number of trade mark applications filed by Hong Kong applicants in other jurisdictions such as Australia, Japan, the European Union, Singapore, the United Kingdom and the United States.

The above statistics suggest that overseas companies are keen to extend the protection of their trade marks to Hong Kong. Similarly, more and more companies in Hong Kong wish to obtain protection of their trade marks in foreign jurisdictions.

JUSTIFICATION FOR APPLICATION OF THE MADRID PROTOCOL TO HONG KONG

The Madrid Protocol currently has 92 contracting parties including the PRC, the United States, the European Union, Australia, Japan, South Korea, Singapore, the Philippines, Vietnam and India. Several ASEAN member states including Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Myanmar and Thailand have also pledged to join the Madrid Protocol by 2015.


One of the perceived benefits of joining the Madrid System for Hong Kong is that it offers a more efficient and cost-effective one stop service for trade mark owners. It makes it easier and indeed encourages local businesses to promote and market their brands overseas and at the same time serves as an incentive for overseas companies to do the same for their brands in Hong Kong. A Government spokesperson said that *“to enhance the competitiveness of Hong Kong as an international business and intellectual property trading hub, the Government believes that it would be in Hong Kong’s overall interest to apply the Madrid Protocol to Hong Kong so that we can take advantage of the Madrid System.”*

TIMETABLE FOR IMPLEMENTATION

The introduction of the Madrid System to Hong Kong will need approval from the Central People’s Government of the PRC.

Under the Basic Law of Hong Kong, the application to Hong Kong of any international agreements to which the PRC is a party shall be decided by the Central People’s Government, in accordance with the circumstances and needs of Hong Kong and after seeking the views of the Hong Kong Government. Therefore, the Hong Kong Government will need to convey the views and suggestions gathered in this consultation exercise to the Central People’s Government and discuss with the relevant PRC authorities about the proposed application of the Madrid Protocol to Hong Kong.

Another step critical for the application of the Madrid Protocol to Hong Kong will be the amendment of the existing Trade Marks Ordinance and Trade Marks Rules of Hong Kong in order to cater for the international registrations regime under the Madrid System.

The current estimate is that it may take some three to four years to complete all these steps. That said, even though it is likely to take at least three to four years before we see the implementation of the Madrid System in Hong Kong, the consultation paper is an important first step, as views from all stakeholders are now sought on this potential landmark change of the trade mark regime in Hong Kong. 



MIIT Issued Draft SMS Rules for Consultation

By Eugene Low, Senior Associate, Mayer Brown JSM, Hong Kong

On 4 November 2014, the PRC Ministry of Industry and Information Technology (MIIT) published for public consultation the *Draft Administrative Rules for Telecommunication Short Message Services* (“**Draft SMS Rules**”). The key objective of the Draft SMS Rules is to reduce the number of spam SMS messages in China. The public consultation ended on 5 December 2014. MIIT has yet to publish the finalised rules.

The volume of spam SMS messages targeting China’s mobile phones have surged in recent years. A recent news report noted that in just the first half of 2013, there were an estimated 200 billion spam messages sent to mobile phones in China. In addition to mobile phone users, Internet users have also fallen prey to spam SMS messages. Tencent, a major IT corporation and the developer of online instant messaging service QQ, reported a total of 356 million junk SMS messages received by its mobile application users in the first half of 2013, 50 million more than that in 2012. The Draft SMS Rules represent the PRC government’s efforts to address these concerns.

We summarise below the main provisions of the Draft SMS Rules:

Regulation on SMS service providers and content providers

- Under the Draft SMS Rules, all SMS service providers must obtain a telecommunications operator licence.
- SMS service providers must include in the message the sender’s genuine phone number or code.
- SMS service providers must keep records of when a message was sent and received and whether the recipient has subscribed for or unsubscribed for its SMS, for a period of 5 months.
- SMS content providers must not distribute SMS messages containing restricted contents as set out under the PRC Telecommunications Regulations
- No person shall employ automated or other means to generate others’ phone numbers for the purpose of sending unsolicited SMS messages.

Restrictions on sending commercial SMS messages

- No person shall send commercial SMS messages without first obtaining the consent of the recipient. Where a recipient has previously given his consent but later chooses to opt out, the content providers must not send further commercial SMS messages to him.
- SMS service providers and content providers who wish to obtain consent from recipients for sending commercial SMS messages must explain to the recipients the type, scope and duration of time of the proposed SMS messages that will be sent to them. Recipients who have not replied to such an invitation will be deemed not agreeing to receive such SMS messages.
- SMS service providers and content providers must include in the SMS messages a free-of-charge and efficient “opt-out” facility to the recipients.



Any individual or organisation who contravenes the above may face a penalty of up to RMB 30,000. MIIT may also make a public announcement about the contravention.

Going forward

The Draft SMS Rules reflect the PRC Government's determination in tackling spam SMS messages in the PRC. We will monitor the progress of the implementation of the draft Rules and keep readers updated. 📶



Banking on Your Personal Data: Recent Guidance Issued to Banks

By Gabriela Kennedy, Partner, Mayer Brown JSM, Hong Kong

Sara Or, Partner, Mayer Brown JSM, Hong Kong

Karen Lee, Associate, Mayer Brown JSM, Hong Kong

Given the private nature of banking services and as banks serve the vast majority of the public, the banking industry is one of the private sectors in Hong Kong for which the Hong Kong Privacy Commissioner receives most complaints. For the same reasons, data privacy compliance by the banking industry attracts particular attention, not only from the regulatory authorities, but also from the public. Due to the sensitive nature of the information handled by the banking industry, the consequences of personal data being mishandled, lost, leaked or stolen can be very serious. The risk is heightened by the increased threat of cyber crime. In October 2014, both the Privacy Commissioner and the Hong Kong Monetary Authority (“**HKMA**”) issued guidelines to banks on how to protect personal data. This article focuses on the handling of customer data by banks.

THE PRIVACY COMMISSIONER’S GUIDANCE NOTE

On 6 October 2014, the Privacy Commissioner issued a Guidance Note on the Proper Handling of Customers’ Personal Data for the Banking Industry (“**PC Guidance Note**”). The PC Guidance Note provides the banking industry with tailored advice on how to ensure compliance with the Personal Data (Privacy) Ordinance (“**PDPO**”). This advice addresses the following aspects:

Personal information collection statements

On or before the collection of a customer’s personal data, a bank is required to notify the customer of certain information in accordance with the PDPO. It is recommended that such notice be provided in the form of a personal information collection statement (“**PICS**”), which can be provided in the application form used to collect the customer’s personal data, or attached to the form as a separate notice. The PICS must specify:

- a. The purposes for which the customer’s personal data may be used;
- b. The classes of persons to whom the customer’s personal data may be transferred;
- c. Whether or not it is mandatory or optional for the data requested to be provided, and the consequences for failing to provide it;
- d. The customer’s right to access and correct his personal data held by the bank, and the name, job title and address of the bank officer who is responsible for handling data access or correction requests.

Banks are advised to communicate effectively the PICS to their customers. The PICS should be in clear and simple language easily readable and understandable, and should also be easily accessible. Banks should therefore take into account the language used and the layout and presentation of the PICS (e.g., simple English or Chinese, reasonable font size, headings to facilitate reading, etc). Banks should ensure that the PICS is presented to customers in a conspicuous manner. They should also consider providing the customers with a help desk or enquiry hotline to assist them in understanding the PICS.

If personal data is collected from a customer over the phone or electronic means, the bank is still required to comply with the PICS requirement. The bank will have to keep good records of having communicated the PICS to a customer before or at the time of collecting his personal data.

Hong Kong Identity Cards (“HKID”)

Banks are required by law and HKMA regulatory guidelines to perform KYC and AML due diligence on customers and potential customers. Banks are therefore allowed by the PDPO to collect their HKID numbers. However, a bank may not collect HKID number from a non-customer, unless otherwise required by law.

For example, a bank is required by the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (“**AMLO**”) to collect the HKID number of a non-account holder when carrying out an “occasional transaction” for them. Examples of an occasional transaction include money changing of an aggregate value of at least HK\$120,000, or wire transfer of an aggregate value of at least HK\$8,000.

Customer records

Banks should take all reasonably practicable steps to ensure that a customer’s contact details are accurate and up-to-date, to ensure that bank statements and other correspondence are not sent to the wrong person. Banks should put in place automated or manual checking procedures to ensure that all information (and variations) provided by the customer from time to time has been correctly entered onto the bank’s records.

Retaining customers personal data

Under the PDPO, a customer’s personal data must not be kept for longer than is necessary. As such, banks should implement clear data retention policy to ensure that personal data is erased after the purposes for which it was collected have been fulfilled. When determining the period of retention, banks should take into account the purposes for which the personal data is to be used and any applicable regulatory or legal requirements on record-retention periods (e.g., Banking Ordinance, AMLO, Securities and Futures Ordinance, Companies Ordinance, Inland Revenue Ordinance, etc.).

Exceptions may also be made where a longer retention period is justified. Examples include where it is necessary to retain the data as it relates to a current or impending legal action or complaint, or is needed to facilitate performance of a contractual obligation.

As regards retention of a customer’s bankruptcy data, the Privacy Commissioner advises banks to retain for no longer than 8 years. The rationale for the 8-year period is that a bankrupt individual would normally be discharged between 4 to 8 years from the commencement of bankruptcy, and so it is not necessary for a bank to retain bankruptcy data for longer than 8 years.

Sharing customers’ personal data within the same banking group

Banks should not allow unrestricted sharing of their customers’ personal data amongst group entities. Intra-group sharing of customer data has to comply with the PDPO. The PICS should inform a customer of the intra-group sharing, and the sharing of data should not be excessive having regard to the purposes for which data is collected and used and other relevant

circumstances. In any other case, a bank is not permitted to share customer data within the group unless with the customer's express consent or unless the bank may rely on a specific exemption in the PDPO.

A bank should establish a group policy on the sharing of customer data. It should also keep up-to-date logs on the transfer of customer data within the group.

Transferring customers' personal data outside Hong Kong

All requirements in the PDPO regulating transfer of personal data apply to a bank transferring customer data, whether within Hong Kong or to a place outside of Hong Kong. In addition, the Privacy Commissioner has been considering an effective date for section 33 of the PDPO. In the meantime, the Privacy Commissioner advises banks to take into account the requirements of section 33 in communicating to customers their practices and arrangements relating to transfer of data if they intend to transfer data outside of Hong Kong.

Disclosing customers' personal data to financial regulators and law enforcement agencies

Even if requested by a governmental agency or regulatory authority to disclose a customer's personal data, a bank should exercise caution and should not make indiscriminate disclosure. Banks should not assume that disclosure requests from governmental agencies or regulatory authorities are automatically and invariably mandatory and binding on banks. Before accommodating a disclosure request, a bank should duly assess the request and determine whether the bank may rely on a legal ground for making disclosure. Typical legal grounds include:

- a. The disclosure is directly related to the original purposes for which the customer data was collected;
- b. The customer has given express consent for disclosure; or
- c. The disclosure is permitted by virtue of a specific exemption in the PDPO, including where the disclosure is required or authorised by law or a court order binding on the bank, or is required in relation to any legal proceedings in Hong Kong.

Using customers' personal data in debt collection

Banks should specify in the PICS that debt collection agents form one of the classes of persons to whom they may transfer customers' personal data. In the absence of that, a bank will have to obtain a customer's express consent before transferring his data to debt collection agents. It is also good practice for a bank to make readily available to a customer of its debt collection policies and practices.

A bank will remain responsible for contravention of the PDPO by its debt collection agents. As such, banks should impose back-to-back contractual obligations on debt collection agents that are consistent with the PDPO and other obligations on the bank. In addition, a bank should not disclose excessive customer data to debt collection agencies.

The same requirements apply with respect to other service providers and data processors appointed by the bank. A bank is required to adopt contractual or other means to manage its service providers and data processors. The PC Guidance Note expressly states that a simple provision requiring a service provider or data processor to comply with the PDPO or the laws of Hong Kong will not exonerate the banks from liability under the PDPO.

Protecting customers' personal data during off-site marketing campaigns

Where banks organise off-site marketing activities to promote their products, this will likely involve the collection of personal data. A bank should implement clear policies and procedures to ensure secure handling of personal data by its marketing staff. The policies and procedures should, among other things, require the staff to keep any forms or documents containing customer data securely stored in a locked container and securely transported to the bank's premises, and prohibit the staff from bringing them home.

Collecting and protecting customers' personal data in e-banking situations

The PC Guidance Note contains advice specifically applicable to e-banking services offered by banks. Particular attention is drawn to the following aspects:

- a. When a customer logs onto a bank's e-banking platform to apply for the e-banking services and provide his personal data on-line, he should be given the PICS before his personal data is collected – the PICS can be given online either on the same webpage or through a prominent link;
- b. Any online form should follow the paper equivalent, and any mandatory items or optional items to be completed should be clearly labelled;
- c. Where cookies are used, it is good practice to disclose the bank's policy regarding cookies, including what kind of information is stored on the cookies and whether a customer may opt out of the cookies and the consequences of opting out; and
- d. It is good practice to inform customers of the specific security measures applicable to online transmission of their personal data.

Handling data access requests

Individuals are entitled to request access to any of their personal data held by the bank. If the bank receives data access request, it is required to respond within 40 calendar days by providing the requested data or notifying the individual that it does not hold his personal data. The bank is allowed to charge a reasonable fee for complying with the data access request, restricting to the direct costs incurred by the bank in complying with the data access request.

Make privacy policies and practices generally available

Banks must take all reasonable practicable steps to ensure that their privacy policies and practices, are accessible by the general public. A banks may post a statement of such policies and practices on its website and include a link on its homepage or other pages where personal data is collected. Such link should be clearly marked, e.g., "Privacy Policy Statement". It is recommended that the privacy policy statement include information such as the kinds of personal data the bank holds, the main purposes for which the data is used, the bank's data retention policy, its data disclosure and transfer policies, etc.

CONSEQUENCES OF BREACHING THE PDPO

Whilst breach of the PC Guidance Note will not in itself constitute an offence, the Privacy Commissioner will take it into account and is likely to weigh unfavourably against the bank in a case or complaint brought before the Privacy Commissioner alleging a contravention of the PDPO.

When the PDPO was amended in 2012, several changes relating to enforcement notices were introduced. More important changes include increased penalties for breaching multiple enforcement notices or for repeated contravention of the PDPO on the same facts after an enforcement notice has been issued and complied with. Further, the Privacy Commissioner is empowered to issue an enforcement notice whether or not the breach is actually continuing or whether or not he is of the opinion that the breach is likely to continue or be repeated (which was a pre-requisite before the PDPO was amended).

THE HKMA CIRCULAR

On 14 October 2014, the HKMA issued a Circular on Customer Data Protection (“**HKMA Circular**”). The HKMA Circular focuses on the controls to prevent and detect loss or leakage of customer data and procedures for addressing and reporting such incidents.

The HKMA expects all authorized institutions to complete a critical review of the adequacy and effectiveness of their existing controls and procedures by the first quarter of 2015. In conducting the review, an AI should have regard to the guidance provided in the HKMA Circular and other applicable guidance issued by the HKMA. If the review reveals weakness or areas for improvements, the HKMA expects an AI to implement appropriate measures promptly to strengthen the controls

Major aspects addressed by the HKMA Circular include the following:

- a. Appoint a designated senior officer or committee to oversee the protection of customer data, and the handling and reporting of any loss or leakage of customer data;
- b. Classify customer data according to its sensitivity and risk level, and put in place security controls based on the assessed risk levels;
- c. Have in place policies and procedures covering system controls, physical security controls, mobile computing, etc.;
- d. Implement an awareness programme to remind staff members at least annually of:
 - The importance of complying with the AI’s data security policies and procedures;
 - Their obligation to promptly report any data leak or loss of data; and
 - The disciplinary actions that may be taken against staff members for violation of the internal security policies and procedures, or failure to report a data leak or loss;
- e. Have in place access controls to prevent any unauthorised access of customer data, including restricting access to designated staff members on a need-to-know basis; disabling and preventing the use of tools to download massive amounts of data, unless management approval has been obtained, etc;
- f. Have in place controls over the transmission of customer data to external networks and systems, including implementing strong data encryption, preventing access to Internet services that can store data (e.g., external email accounts, cloud service) or file-sharing software, and having controls to detect suspicious activities, such as any massive downloading of data;
- g. Control the ability of staff members to store customer data on portable storage devices, including:
 - Restricting or preventing the use of portable storage devices;
 - Deploy password protect and data encrypt portable storage device and backup tapes;
 - Record the use of portable storage devices;

- Record the reporting of any loss of a portable storage device;
 - Erase data from the portable storage device when no longer needed;
- h. Ensure the secure disposal or destruction of customer data stored on paper or any other media;
 - i. Control the use of personally owned computer devices by staff members in relation to their employment (i.e., “Bring Your Own Device” policy):
 - Staff members should generally only use devices provided by and owned by the AI;
 - However, if an AI has a “Bring Your Own Device” policy, it should comply with the Hong Kong Association of Banks’ standards on minimum controls;
 - j. Implement physical security controls where customer data is stored, and whenever customer data is being relocated or transported, including security guards, CCTV, etc;
 - k. Engage independent third parties to conduct periodic audits on the adequacy of and compliance with the AI’s controls over customer data;
 - l. Have in place controls over the handling of customer data by third party service providers, including imposing contractual obligations on them to comply with the AI’s policies and procedures; and
 - m. Report any loss or leakage of customer data to the HKMA, the relevant customers and the Privacy Commissioner where appropriate. The HKMA expects an AI to provide justification for a decision not to report.

Banks should complete the critical review by Q1 2015 in accordance with the HKMA Circular and take necessary and timely steps in light of the results of the review.

CONCLUSION

Banks are under increased scrutiny from the Privacy Commissioner and HKMA, as well as the general public. There is also heightened expectation for banks to treat data protection as an integral part of their overall compliance infrastructure.

The potential consequences of non-compliance include investigations, fines, civil claims and reputational damage. It is therefore very important for a bank to design and implement an effective data protection compliance policy that addresses all legal and regulatory requirements from various sources that are applicable to it having regard to the nature and scale of business, and its circumstances and needs. For a bank that is part of an international group, the compliance policy will have to address not only requirements under Hong Kong law but also foreign laws and group policies. Apart from management commitment and oversight, a key component of the compliance policy is staff awareness and training.

Whilst cyber security and employee data handling are beyond the scope of this article, we have designated teams and experts to provide advice on those topics. Please contact us if you require further assistance. ☎



To Search or Not to Search? Does the Right to Privacy Prevent the Police from Seizing and Searching Mobile Phones in Hong Kong?

By *Gabriela Kennedy, Partner, Mayer Brown JSM, Hong Kong*
Karen Lee, Associate, Mayer Brown JSM, Hong Kong

A protester who participated in the July 1 march this year has made headlines by filing an application for leave to apply for judicial review before the Court of First Instance in Hong Kong for breach of his right to privacy¹. The breach relates to police officers searching mobile phones incidental to an arrest without a warrant. This, according to the application for leave, is unconstitutional and a breach of a person's right to privacy.

BACKGROUND

On 4 July 2014, four protesters were arrested by the police in connection with an alleged offence that occurred during the July 1 protest in Hong Kong. Police officers seized and briefly inspected the mobile phones of the protesters without a warrant, on the basis that the mobile phones were required as part of their investigation to determine whether or the protesters had collaborated in the alleged offence.

On 3 October 2014, one of the protesters (the “**Applicant**”) filed an application for leave to apply for judicial review before the Court of First Instance (the “**Judicial Review**”), seeking (amongst other things):

- a. A declaration that Section 50(6) of the Police Force Ordinance (Cap. 232) (“PFO”) does not authorise police officers to search the contents of mobile phones seized on arrest;
- b. If it is found that Section 50(6) of the PFO does empower police officers to search the contents of mobile phones without a warrant, a declaration that such power is unconstitutional and inconsistent with Article 14 of the Hong Kong Bill of Rights and Article 30 of the Basic Law of Hong Kong;
- c. An order that the decision of the police officer to seize the mobile phones for the purpose of searching their contents be brought up and quashed; and
- d. An expedited hearing of the application.

This is the first case brought in Hong Kong based on an allegation of infringement of an individual's right to privacy under the Basic Law and the Bill of Rights.

RIGHT TO PRIVACY

Article 30 of the Basic Law and Article 14 of the Bill of Rights grants Hong Kong residents the right to freedom and privacy of communication, and to not be subjected to unlawful or arbitrary interference with his privacy or correspondence. The only exception is where the relevant authorities must inspect personal communications, in accordance with legal procedures, in order to meet the needs of public security or to investigate a criminal offence.

¹ HCAL 122/2014

Under Section 50(6) of the PFO, the police are empowered to seize, without a warrant and during a person's arrest, any "newspaper, book or other document...or any other article or chattel" that is found on such person or in the place he is arrested. The Applicant argues that the correct interpretation of this Section does not include the right to search the contents of mobile phones seized on arrest. Even if Section 50(6) of the PFO is found to have granted this power to the police, the Applicant still maintains that without a warrant such exercise of power is unconstitutional and infringes the Applicant's fundamental right to privacy under the Basic Law and the Bill of Rights.

MOBILE PHONES

The amount of information that can be stored and accessed on a mobile phone, especially a smartphone, is substantial and will inevitably contain personal data, e.g., email correspondence, instant messages, social networking content, photographs, Internet browsing history, location history and even credit card information where the mobile is used for, say, NFC payments. Mobile phones may even contain content that is subject to legal professional privilege. The modern mobile phone is essentially comparable to a computer. In fact, the Hong Kong courts have previously determined that a mobile phone should be treated as a computer due to the functions and level of information that can be stored on a mobile phone².

Any review of the information stored in a mobile phone will therefore be highly intrusive, and will give the police access to a substantial amount of information, most of which is unlikely to be relevant to the investigation. As stated by the Applicant in his application for Judicial Review:

"mobile phones are markedly different in nature from other documents, articles or chattels that may be found on an arrestee's person or in a place of arrest...searches of digital data stored on mobile phones cannot be treated as comparable with searches of physical items that may be found on an arrestee's person".

The Applicant argued in his application for Judicial Review that whilst a police officer may seize a mobile phone upon a person's arrest in order to ensure the integrity of the data, the police officer should not be able to search the content of the phone without first obtaining a warrant – to allow otherwise would amount to a disproportionate interference with the person's right to privacy.

CONFLICTING INTERESTS

There is a clear conflict between a person's right to privacy versus a police officer's duty to investigate and prosecute offenders. The goal is to achieve a balance, which is in the best interests of the public.

Whilst it may be argued that the police can simply secure a mobile phone in order to protect its contents from being erased, and to then obtain a warrant in order to review the information stored on it, the latest developments in technology mean that offenders can remotely wipe the data on their mobile phones whilst they are in police custody. There is therefore a risk that key

2 See *Secretary for Justice v Wong Ka Yip Ken* (HCMA 77/2013) and our previous article entitled "How Smart is a Smartphone and How about its User?": http://www.mayerbrown.com/files/Publication/8eb13951-767e-47cf-ae1d-5f7e713d8958/Presentation/PublicationAttachment/8d26ced7-6527-4470-8a78-711e3e60818c/IP-%26-TMT-Quarterly%20Review_Q42013.pdf

evidence may be deleted before the police have a chance to discover it. One way to overcome this is for the police to place the mobile device in a radio-frequency shielded bag to prevent the data from being compromised, rather than in a microwave, which apparently is also an effective means of blocking any attempts to remotely erase its contents.

On the other hand, the risk associated with providing the police with unrestricted access to an arrestee's mobile phone is illustrated in a currently ongoing U.S. case where an individual has brought an action against the U.S. government for creating a Facebook page containing photographs of her obtained from her mobile phone. The U.S. Department of Justice had arrested the plaintiff in July 2010 in relation to a drug charge. At the time of her arrest, she had surrendered her mobile phone and consented to the police officers accessing its content in order to assist in a related criminal investigation. As part of this investigation, the police created a fake Facebook page in the name of the plaintiff, and included photos of her, her son and her niece. The plaintiff is therefore suing the U.S. government for breach of her right to privacy. The U.S. government argue that the plaintiff had "relinquished any expectation of privacy she may have had to the photographs on her cell phone" when she agreed to let police officers search and use information on the device³.

OTHER JURISDICTIONS

The question of a person's right to privacy versus a police officer's right to conduct a warrantless search has also been considered in other common law jurisdictions. For example, in Canada and the U.S. the courts currently appear to take the view that searching an individual's mobile phone upon their arrest without first obtaining a warrant, will in certain circumstances violate the individual's right to privacy against unreasonable searches and seizures⁴. In particular, it was recognised by the Canadian courts that due to the quantity and quality of personal data that may be contained in a mobile phone, any search conducted by the police of the entire content of a phone would be highly invasive and should therefore not be conducted without a warrant⁵.

In the U.S., it was recently held that searching a mobile phone without a warrant will generally be found to be unreasonable as:

- a. It is not justified in order to protect the safety of the police officers (e.g., a phone cannot be used as a weapon) or necessary in order to preserve evidence; and
- b. More substantial privacy interests are at stake in relation to searching the content of a mobile phone due to the level of information that may be accessed (e.g., even information not stored on the mobile device itself but, say, in the cloud, could be searched via the mobile phone).

The Applicant in his application for Judicial Review submits that the above reasoning applied in the Canadian and U.S. courts should be similarly applied in Hong Kong.

³ *Sondra Arquiett v. United States of America et al* (Civil Action No. 13-CV-0752 (TJM/TWD)),

⁴ *Riley v. California*, 573 US (2014); *R v. Mann*, 2014 BCCA 231

⁵ *R v. Mann*, 2014 BCCA 231. However, although the court found that Canadian law does not allow police to conduct a warrantless search of the entire contents of a person's mobile phone, the admission of the evidence obtained from searching the phone would not bring the administration of justice into disrepute and so the evidence was not excluded.

However, it should be noted that the Canadian Charter and U.S. Constitution make direct references to unreasonable searches and seizures, whereas Hong Kong's constitution merely refers to "legal procedures" and "unlawful interference". The Canadian Charter provides that "everyone has the right to be secure against unreasonable search and seizure", and the U.S. Constitution provides that a person's right "to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause...and particularly describing the place to be searched, and the persons or things to be seized."

In contrast, the Hong Kong Basic Law provides that a person's freedom and privacy of communication may not be infringed "except that the relevant authorities may inspect communication in accordance with legal procedures to meet the needs of public security or of investigation into criminal offences". The Hong Kong Bill of Rights also goes on to provide that no one may be subject to "arbitrary or unlawful interference with his privacy, family, home or correspondence". However, what if the current law and legal procedure itself is seen to be excessive and an infringement of a person's right to privacy, as is alleged by the Applicant in the Judicial Review?

The fundamental question, therefore, is what amounts to a legal search and seizure in Hong Kong and, if the search and seizure was in accordance with the legal procedure, can this still be said to be unconstitutional?

CONCLUSION

How far will the courts go to protect an arrestee's right to privacy? Does the amount of information on a smartphone mean that a search of the contents by the police will be highly intrusive? Does the intrusive nature of such a search mean that police should be obligated to obtain a warrant prior to searching an arrestee's smartphone? All will be revealed once the Judicial Review is concluded. 📶



The Future of Innovative Payments

[This article first appeared in the *E-Finance & Payments Law & Policy* (Nov 2014 issue)]

By Gabriela Kennedy, Partner, Mayer Brown JSM, Hong Kong

Karen Lee, Associate, Mayer Brown JSM, Hong Kong

Mobile payments and PayWave machines are just some of the new ways for consumers to pay for goods and services in Hong Kong. The rise in these new methods of payment led to the proposal by the Financial Services and Treasury Bureau (“**FSTB**”) and the Hong Kong Monetary Authority (“**HKMA**”) of a new regulatory regime outlined in their public consultation paper issued on 22 May 2013 (“**Consultation Paper**”). The consultation period ended on 22 August 2013. More than a year later, on 31 October 2014, the FSTB and HKMA issued the Consultation Conclusions summarising the comments received from market players and government bodies. These conclusions are discussed below.

THE NEW LEGAL FRAMEWORK

Under the Consultation Paper, the FSTB and HKMA invited public comments on the introduction of a new legal framework to regulate stored value facilities (“**SVFs**”) and retail payment systems (“**RPSs**”).

An RPS is a system for the transfer, clearing or settlement of low-value payments for retail purchases, e.g., mobile payments, credit cards, etc. An SVF involves the pre-payment to or storage of the value of money on a payment facility, e.g., a gift card. An SVF can be categorised as:

- i. A single-purpose SVF (which can only be used to purchase goods or services from a single merchant, e.g., a gift card) or a multi-purpose SVF (which can be used to obtain goods or services from multiple merchants, e.g., the Octopus card); and
- ii. Device based (where value is stored on a physical device) or non-device based.

Currently, only multi-purpose device based SVFs are regulated under the Banking Ordinance – non-device based SVFs and single-purpose SVFs are not subject to mandatory regulations under Hong Kong law. Similarly, RPSs are not regulated but a voluntary “Code of Practice for Payment Card Scheme Operations”, which sets out general principles to promote safety and efficiency of payment card operations, was adopted by 8 card operators in 2007 and endorsed by the HKMA.

Under the new proposed regulatory regime set out in the Consultation Paper both device based and non-device based SVFs and RPSs will be regulated via amendments to the current Clearing and Settlement Systems Ordinance (“**CSSO**”), and the existing multi-purpose SVF regime under the Banking Ordinance will be migrated to the CSSO. In short, the Consultation Paper proposed that:

1. All issuers of multi-purpose SVFs in Hong Kong (whether device or non-device based) would be required to obtain a licence from the HKMA before issuing the SVF;
2. Single-purpose SVFs would not be regulated under the proposed regime;
3. Licensed banks in Hong Kong will be deemed to already have a licence to issue multi-purpose SVFs, and therefore would not need to obtain a separate SVF licence;

4. Issuers of multi-purpose SVFs (other than licensed banks) would be required to keep the float separate from their own funds, which would have to be fully protected by certain safeguarding measures;
5. The HKMA would have the power to designate certain types of RPSs which would be subject to the HKMA's continuous oversight;
6. An RPS would only be designated for oversight if: (i) it is operated in Hong Kong or processes Hong Kong dollars or any other currencies prescribed by the HKMA; (ii) the disruption of the business of such an RPS would have an impact on Hong Kong's financial stability, the day-to-day commercial activities in Hong Kong, or would undermine public confidence in Hong Kong's payment of financial systems; and
7. If the HKMA believes that an offence has been committed under the new regime (e.g., a person has operated an SVF without a licence or contravened a licensing condition, etc), the HKMA will have the power to direct an investigator to conduct an investigation; to compel the provision of evidence by the alleged offender; and to apply for search and seizure warrants.

For a more detailed analysis on the new legal regime proposed by the FSTB and HKMA please see our previous article *"Aligning the law with innovative payments in Hong Kong"* published in the E-Finance & Payments Law & Policy in October 2013.

THE CONSULTATION CONCLUSIONS

The FTSB and HKMA received 41 submissions from various market players and government bodies, including the Consumer Council, the Hong Kong Association of Banks, Alipay, Tencent, PayPal, Visa, MasterCard, Deloitte and KPMG. The submissions were summarised by the FTSB and HKMA in its Consultation Conclusions issued on 31 October 2014.

The submissions indicate overall support for the policy objectives and main proposals in the Consultation Paper. Most of the market players and government bodies who submitted a response believe that introducing a regulatory regime will further foster the development of retail payment products and services, and will encourage user confidence. However, a number of concerns were raised regarding particular elements of the proposal. The major comments are outlined below, along with the responses from the FTSB and HKMA (the "government") as set out in the Consultation Conclusions:

Licensed banks deemed to have an SVF licence

The Consultation Paper proposed that licensed banks would be deemed to be licensed for multi-purpose SVFs. Unlike other players, licensed banks would not be required to ensure that the float is kept separate from other funds and would not be required to implement certain safeguarding measures to protect the float.

Some of the non-bank respondents were of the view that this proposal gave banks a competitive advantage, and that banks and non-banks should be subject to the same regulatory requirements in order to maintain consistency in the market and a level playing field for all parties.

The original proposal under the Consultation Paper has been maintained, namely that licensed banks will be deemed to be licensed to issue SVFs. The rationale for this is that licensed banks are already subject to stringent requirements and the ongoing supervision of the HKMA.

However, to ensure consistency, the government agreed that both banks and other SVF licencees should be required to observe the same float safeguarding principles, which are as follows:

- a. To have in place float protection measures that adequately protect the float; and
- b. To keep the float separate from the issuer's other funds.

An SVF issuer will need to demonstrate to the HKMA's satisfaction that their float safeguarding measures provide adequate protection.

Definition of SVFs and scope of application

The Consultation Paper proposed that the definition of SVFs should include "money's worth", so that it would capture the concept of "value", i.e., real money as well as other forms of monetary consideration that can be redeemed by an SVF user, or value added into an SVF account by a user or received from another person.

Some of the responses received raised concerns over the fact that too broad a definition would encompass things such as:

- a. Air mileage schemes, loyalty schemes and bonus points schemes; and
- b. Prepaid cards or coupons (e.g., gift cards) issued by a single online store platform (e.g., Amazon), which are used to purchase digital products (e.g., music, e-books, etc), whose intellectual property is owned by different third parties.

Such items should not be captured by the regulatory regime as they posed minimal risk to users.

While noting that the examples given by the respondents are more likely to fall under the single purpose SVF, which is not regulated, the government proposed further amendments to the definition of SVFs, in order to exclude:

- a. Any bonus or loyalty point scheme, even if a small portion of the points can be purchased by users in cash;
- b. Any facility that can be used within one or more of the issuer's premises (e.g., department store), so long as the total float does not exceed HK\$ 1 million; and
- c. Any facility which can only be used within specified premises and which relates to a specific person (e.g., recreational clubs, university campuses), and the total float size does not exceed HK\$ 1 million.

Separate SVF licences for issuers and facilitators

The Consultation Paper proposed that separate licences would need to be obtained if a company wished to issue SVFs and to facilitate the issuance of SVFs.

A few responses noted that a company which is licensed to issue SVFs, should not have to apply for a separate licence to facilitate the issuance of SVFs, and vice versa.

The government has agreed to unify the licensing process so that companies need only obtain one licence in order to be able to act as an SVF issuer and an SVF facilitator.

Maximum value to be stored on SVFs

The Consultation Paper proposed that the maximum amount that can be stored on a multi-purpose SVF is HK\$ 3,000.

The concerns expressed in relation to the maximum value proposed were that the HK\$ 3,000 threshold was too low in relation to non-device based SVFs, which normally involve the receipt of money as well as the making of payments. Some respondents suggested that a risk based approach should be adopted in respect of non-device based SVFs.

In response to these concerns, the government has agreed that the HK\$ 3,000 limit should only apply to device based SVFs. By contrast, a risk-based approach to be assessed on a case-by-case basis, should be adopted for non-device based SVFs.

Single-purpose SVFs

The Consultation Paper proposed that single-purpose SVFs (e.g., pre-paid gift coupons or gift cards) would not be subject to the regulatory regime.

A few of the respondents (including the Consumer Council) noted that single-purpose SVFs should be regulated, as some single-purpose SVFs may accumulate a substantial float received from a large number of users. Dissenting views were offered by the Hong Kong Bar Association and the Hong Kong Association of Banks.

Despite submissions to the contrary, the government maintained the original position that single-purpose SVFs should not be regulated, as they pose a limited risk to consumers and would stifle business innovation.

Physical presence in Hong Kong and minimum capital

The Consultation Paper proposed that applicants would be required to meet certain conditions in order to obtain and maintain an SVF licence. These include having a physical presence in Hong Kong, the principal business being the issuance of or facilitating the issuance of SVFs, and a minimum on-going capital requirement of at least HK\$ 25 million.

Such requirements do not take into account the fact that some overseas SVF issuers are already subjected to sufficient supervision in their home country and can show that they have adequate float safeguarding measures. They should therefore be exempt from the requirement to have a local presence in Hong Kong and to comply with the float safeguarding requirements. Views were also expressed that the minimum HK\$25 million on-going capital requirement was too high.

Given that the intention was to ensure that the HKMA can exercise day-to-day supervision over the issuers, and they should exist as stand-alone entities separate from their affiliated overseas businesses, these concerns were not entertained. The HK\$25 million threshold was also considered to be consistent with the current multi-purpose SVF regime under the Banking Ordinance.

Designating RPSs

The Consultation Paper proposed that the HKMA would have the right to designate RPSs that are to be monitored by it.

As noted above, RPSs are not regulated in Hong Kong; there is instead voluntary self-regulation. The Consultation Paper envisaged that the HKMA would have the power to designate RPSs it wishes to regulate and that such regulation would be derived from the existing rules under the CSSO. Concerns were expressed that subjecting credit card schemes to the RPS regulatory framework would undermine Hong Kong's status as an international financial centre, and that the existing self-regulation by payment card operators is sufficient to protect consumers.

Again, the government was not persuaded by these submissions and the original proposal, which is believed to be in line with international regulatory trends, will be maintained.

THE WAY FORWARD

Now that the FSTB and HKMA have got the ball rolling there is no turning back. A bill to amend the CSSO is being drafted. The plan is to introduce it to Legislative Council in the 2014-2015 legislative session. The government has suggested that once the amendment bill is enacted, a transitional period of 12 months will be provided to enable existing SVF issuers to apply for SVF licences. ☺



Recent Changes to the Toys and Children’s Products Safety Ordinance

By Eugene Low, Senior Associate, Mayer Brown JSM, Hong Kong

The Toys and Children’s Products Safety Ordinance (Cap. 424, Laws of Hong Kong) (“**Ordinance**”) was amended on 1 July 2014 to expand the scope of children’s products covered by the Ordinance and impose additional safety requirements in relation to the use of phthalates in toys and children’s products. Coming into operation on the same date were the Toys and Children’s Products Safety (Additional Safety Standards or Requirements) Regulation (“**Regulation**”) and a set of Guidelines published by the Hong Kong Customs and Excise Department (“**Guidelines**”) who is responsible for enforcing the Ordinance.

Expanded definition of “children’s products”

Before the amendment, the Ordinance regulated the safety of “toys” (defined as products or materials that are designed or clearly intended for use in play by a child, and their packaging) and certain “children’s products” specified in Schedule 2 of the Ordinance, namely, babies’ dummies, baby walking frames, bottle teats, bunk beds for domestic use, carry cots and similar handled products and stands, child safety barriers for domestic use, children’s cots for domestic use, children’s high chairs and multi-purpose high chairs for domestic use, children’s paints, children’s safety harnesses, playpens for domestic use, and wheeled child conveyances.

The amended Ordinance has expanded the definition of “children’s products” to include, in addition to those children’s products specified in Schedule 2, “*any product or material which is intended to facilitate the feeding, hygiene, relaxation, sleep, sucking or teething of a child under 4 years of age and contains any plasticised material*”, as well as its packaging.

Examples of products which were not regulated under the old law but would now fall under the new statutory definition include bibs, feeding bottles, cutlery, changing mats, blankets, pillows, sipper cups, straws, gum soothers, etc.

Control of use of phthalates

To ensure that the Hong Kong regime is on par with other advanced economies in protecting children from health hazards attributable to excessive exposure to phthalates, the Ordinance introduced limits on the concentration of six types of phthalates used in toys and children’s products. These six types of phthalates are:

- Benzyl butyl phthalate (BBP);
- Dibutyl phthalate (DBP);
- Di(2-ethylhexyl) phthalate (also known as bis(2-ethylhexyl) phthalate or diethylhexyl phthalate) (DEHP);
- Diisodecyl phthalate (DIDP);
- Diisononyl phthalate (DINP); and
- Di-n-octyl phthalate (DNOP).

The Regulation and the Guidelines set out the detailed numerical concentration limits for these six types of phthalates. For instance, the total weight of Class 2 phthalates (DIDP, DINP and DNOP) in a toy or children’s product or any part which is capable of being entirely or partly

placed in the mouth of a child under 4 years of age must not exceed 0.1 per cent of the total weight of the corresponding plasticised materials. Under the Regulation, a toy or children's product will be considered capable of being placed into the mouth of a child under 4 years of age if:

- a. Each dimension of the toy or product is less than 5 cm; or
- b. The toy or product can, in a reasonably foreseeable manner, be brought to the mouth of such a child and kept in the mouth so that the toy or product can be sucked or chewed.

The Guidelines provide examples of how a toy or children's product may be regarded as capable of being placed into a child's mouth. A "reasonable person" test would be adopted. For example, the seat back and footrest of a baby high chair cannot reasonably be foreseen to be placed into a child's mouth for sucking or chewing.

Enforcement

Under the Ordinance, manufacturers, imports and suppliers (including retailers) all have a duty to ensure that the toys or children's products they deal with (or distribute as prizes or souvenirs for commercial purposes) comply with the safety requirements under the Ordinance, including the new requirements in relation to the use of phthalates, as well as existing requirements as to identification markings and safety warnings for certain classes of toys and children's products. Contravention of the Ordinance may result in warning notices issued by Customs, and/or maximum penalties of a HK\$100,000 fine or 1-year imprisonment on first conviction.

While a person such as a retailer may have a potential defence under the Ordinance if he can show that he has taken all reasonable steps and exercised all due diligence to avoid committing an offence, given that it is the safety of children which is at stake, it is advisable for all who deal with toys and children's products in Hong Kong to familiarise themselves with the new requirements of the Ordinance and take proper measures (including retaining the relevant safety and laboratory records from manufacturers and factories) to ensure compliance. ☺

CONTACT US



GABRIELA KENNEDY

Partner

+852 2843 2380

gabriela.kennedy@mayerbrownjism.com



ROSITA LI

Partner

+852 2843 4287

rosita.li@mayerbrownjism.com



BENJAMIN CHOI

Partner

+852 2843 2555

benjamin.choi@mayerbrownjism.com

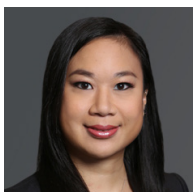


SARA OR

Partner

+852 2843 2268

sara.or@mayerbrownjism.com



KAREN LEE

Associate

+852 2843 4452

karen.hf.lee@mayerbrownjism.com

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

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

This publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is intended to provide a general guide to the subject matter and is not intended to provide legal advice or be a substitute for specific advice concerning individual situations. Readers should seek legal advice before taking any action with respect to the matters discussed herein. Please also read the Mayer Brown JSM legal publications Disclaimer.

Mayer Brown is a global legal services provider comprising legal practices that are separate entities (the "Mayer Brown Practices"). The Mayer Brown Practices are: Mayer Brown LLP and Mayer Brown Europe-Brussels LLP, both limited liability partnerships established in Illinois USA; Mayer Brown International LLP, a limited liability partnership incorporated in England and Wales (authorized and regulated by the Solicitors Regulation Authority and registered in England and Wales number OC 303359); Mayer Brown, a SELAS established in France; Mayer Brown JSM, a Hong Kong partnership and its associated legal practices in Asia; and Tauil & Chequer Advogados, a Brazilian law partnership with which Mayer Brown is associated. Mayer Brown Consulting (Singapore) Pte. Ltd and its subsidiary, which are affiliated with Mayer Brown, provide customs and trade advisory and consultancy services, not legal services.

"Mayer Brown" and the Mayer Brown logo are the trademarks of the Mayer Brown Practices in their respective jurisdictions.

© 2014 The Mayer Brown Practices. All rights reserved.

