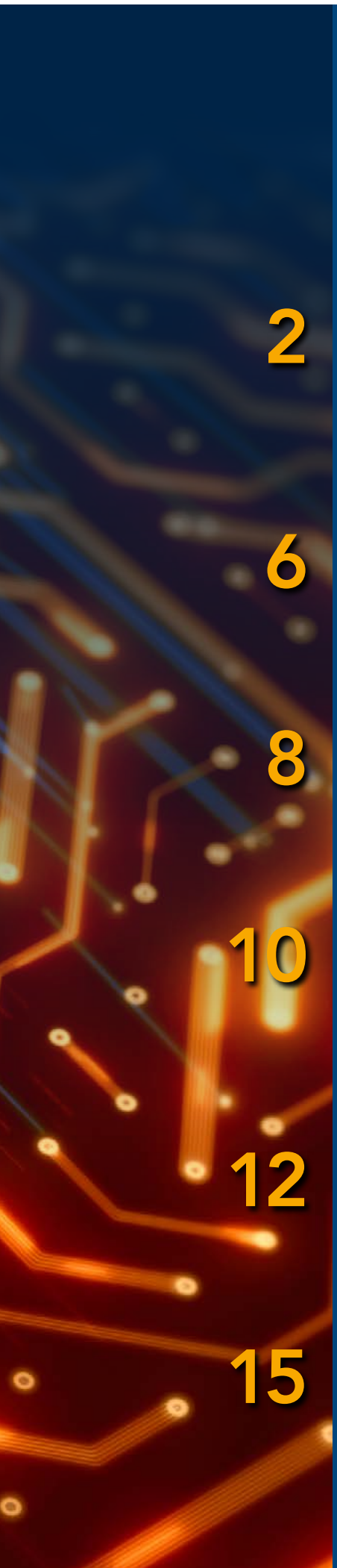
MAYER | BROWN

IP & TMT Quarterly Review

Third Quarter 2020

Contents



The Chamber of No Secrets: What Tech and Data/Content Driven Companies Need to Know About the Hong Kong National Security Law

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

Karen H. F. Lee, Counsel
Mayer Brown, Singapore

Cheng Hau Yeo, Associate
Mayer Brown, Singapore

Introduction

On 30 June 2020, the *Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region* ("**NSL**") was passed by the Standing Committee of the National People's Congress in China and officially listed in Annex III of the Hong Kong Basic Law. It came into effect in Hong Kong on the same date – a day before the 23rd anniversary of the transfer of sovereignty over Hong Kong from the UK back to the PRC. The NSL was enacted in the aftermath of a year of social unrest in Hong Kong and introduced criminal sanctions against acts of secession, subversion, terrorism, and collusion with foreign or external forces. The NSL aims to regulate behaviour through increased scrutiny but its knock-on effects, including the almost immediate response from the US, will likely give rise to far-reaching consequences for the technology and

service sectors given the introduction of new export sanctions for Hong Kong, the increased powers of local enforcement authorities to gain access to data as well as other trade issues that will affect the way technology companies and other businesses operate in the region.

Highlights of the NSL

The key features of the NSL can be summarised as follows[1]:

- The NSL criminalises acts of secession, subversion, terrorism, and collusion with foreign or external forces. Convictions under any of these provisions carry different sentences up to life imprisonment;
- Incorporated or unincorporated bodies, for example, companies and organisations, can be held accountable for violations of the NSL, and penalties may be imposed on them, ranging from fines to confiscation of assets;
- Law enforcement bodies are empowered to take enhanced measures when handling offences that endanger national security, such as searching relevant premises and electronic devices that may contain evidence of the offence, carrying out lawful interception and surveillance, and requiring service providers or individuals to remove information and provide assistance;
- The city's new security office, staffed with its own law enforcement personnel from Beijing, has the power to refer certain serious or complex cases for trial in the PRC;
- The Committee for Safeguarding National Security ("**Committee**"), comprised of Hong Kong government officials and a Beijing-appointed adviser, is in charge of enforcing the NSL in Hong Kong. Decisions made by the Committee are not subject to judicial review; and
- The final right to interpret the NSL is vested in the PRC's Standing Committee of the National People's Congress, and any conflict or inconsistency between the NSL and the laws of Hong Kong will be resolved in favour of the former.

The NSL purports to have extra-territorial effect and does not just apply to offences committed in Hong Kong, or by Hong Kong permanent residents outside Hong Kong, but also applies to any offences committed outside the region by anyone who is not a Hong Kong permanent resident.

Effects of the NSL on Businesses

The new regime introduced by the NSL will require Hong Kong technology companies to consider their obligations to provide access to data and assistance to law enforcement authorities; review their cross-border data flows and restructure their business given changes to technology export controls.

(I) ACCESS TO DATA

Cases concerning an offence endangering national security allow law enforcement authorities to require access to data held by service providers as well as the deletion of certain information in the context of general assistance with an investigation. Enforcement authorities can order any person who is reasonably suspected to have any information relevant to an investigation, to furnish such information, and they have the power to search any premises or electronic devices which may contain evidence of an offence, without a warrant. How unfettered are these powers? Can enforcement authorities request access to all data, or must they specify the exact data they require? What is the threshold for the enforcement authorities to be able to order the provision of information or to carry out searches – is it low or high? What are the consequences for companies that do not comply with an order, especially if they are not based in Hong Kong or if their data is stored in the cloud? Fines, revocation of business licence or imprisonment? The answers to these questions are not clear at the moment and further implementation rules will likely be issued to provide clarification.

What is clearer, though, is that the focus of these wide reaching powers will likely be data centre

1 For further information on the National Security Law, please refer to the following: https://www.mayerbrown.com/en/perspectives-events/publications/2020/07/hksar-national-security-law#:~:text=It%20is%20stipulated%20under%20the,be%20guilty%20of%20an%20offence.

providers, internet service providers, other network operators, mobile app operators and social media platforms which hold a broad range of data on their customers and users, and operate in Hong Kong. For this reason, technology companies operating in Hong Kong need to establish a response plan on how to handle requests from the enforcement authorities. In particular, as the NSL allows police officers to search premises and electronic devices on which evidence relating to an offence may be stored, the risk of dawn raids has to be considered. A good starting point for any company is to assess their potential exposure to such risks and develop a comprehensive playbook setting out appropriate protocols that would need to be adhered to when a dawn raid happens. This will help minimise business disruption and ensure a well-coordinated response.

As part of developing their response playbooks, companies may wish to re-assess and re-evaluate their supply chains and consider adopting solutions that ring-fence their operations in Hong Kong from their global networks.

(II) DATA FLOWS

In early 2019, a bilateral free trade agreement ("**FTA**") was entered into between Hong Kong and Australia, under which Hong Kong committed to allow free cross-border data flows between the two territories. This was the first time Hong Kong had made such a commitment with a trading partner. However, the promulgation of the NSL and recent moves by sovereign states in response to the passing of the NSL are likely to result in a review of such FTAs. Any existing business contracts that rely on provisions under an FTA (or any other bilateral agreements) may need to be reviewed and attendant risks would need to be re-assessed, and pre-emptive changes should perhaps be considered.

(III) TRADE AND EXPORT CONTROL

Since the passing of the NSL, the US government has announced that it will strip away Hong Kong's special trading status and suspend existing licensing exceptions for the export, re-export and transfer of certain controlled technology products to the region.[2] Previously, Hong Kong enjoyed preferential treatment from the US pursuant to the United States-Hong Kong Policy Act, on the condition that Hong Kong would maintain a sufficient degree of autonomy from the PRC. This included export licensing exceptions whereby US companies could be exempted from acquiring a licence for exporting, re-exporting and transferring sensitive and high-technology products falling under the Export Administration Regulations ("**EAR**"), items that would otherwise require an export licence, to Hong Kong. These exceptions were not extended to the PRC.

As a result of the suspension of licensing exceptions, all exports, re-exports and transfers of such classified products to Hong Kong will now be treated as items destined for the PRC, and US companies will be restricted from selling sensitive technology products (e.g., dual-use technologies and defence equipment) to Hong Kong. Similarly, the EU Council has recently released a draft document proposing the implementation of limits on the export of goods to Hong Kong that could be used for surveillance purposes. The proposal is likely to be put into effect in the near future.

The tightened restrictions on sensitive technology exports could have larger implications for multinational companies, such as semiconductor manufacturers, which will now be precluded from shipping sensitive and high-technology products to or receiving them in Hong Kong. Companies that have previously been leveraging Hong Kong's favourable export control status may now have to carefully review their current compliance policies and procedures for importing and exporting controlled technology items subject to the EAR, and carry out the necessary changes to prepare for the potential disruptions to their operations in Hong Kong. This may include reviews of existing contractual obligations for the supply of technology by building in the additional time needed to obtain export licences and/or seeking partnerships with local technology suppliers in order to maintain service levels for Hong Kong customers.

Customers in Hong Kong relying on such technology that may suffer business disruptions may now have to re-assess their options and adopt alternatives such as embracing different technology

2 For further information regarding the revocation of Hong Kong's preferential status by the U.S., please refer to the following: https://www.mayerbrown.com/en/perspectives-events/publications/2020/07/president-trump-revokes-preferential-treatment-for-hong-kong.

solutions and reducing their reliance on US companies by partnering with Chinese companies instead, which are expected to gain a stronger foothold in the Hong Kong market. Maintaining a Hong Kong customer base will require a delicate balancing act on the part of technology companies that now have to contend with new export controls and the threat of access to customer data.

What's Next?

The ripple effect of the NSL has presented technology companies operating in Hong Kong with additional challenges and hurdles. They will need to revisit and reformulate their overall strategy for Hong Kong, by perhaps adopting a similar strategy to that adopted for their operations in the PRC. Rapidly evolving political developments will reflect the way the NSL is enforced and will have a knock-on effect on data privacy issues and technology imports and exports. More than ever, technology companies need to be as prepared as possible, by arming themselves with NSL playbooks and enforcement response plans, which will need to be revisited and updated on a continuous basis.

*The authors would like to thank **Sophie Huang**, Intellectual Property Officer at Mayer Brown, for her assistance with research for this article.*

Shop Until You Drop: China's New Code of Conduct on Livestreaming E-Commerce

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

Karen H. F. Lee, Counsel
Mayer Brown, Singapore

On 24 June 2020, the China Advertising Association ("**CAA**") issued the Code of Conduct for Online Livestreaming Marketing Activities ("**Code of Conduct**"). The Code of Conduct came into operation on 1 July 2020 and introduces new restrictions on marketing via livestreaming sessions in an attempt to regulate the country's livestreaming industry that has been booming in the wake of the Covid-19 pandemic.

The livestreaming industry in China has exploded in the last couple of years, with the number of platforms and the amount of revenue generated hitting a record high. In China, 4 million live streaming sessions were reported in the first quarter of 2020[3], and live streaming e-commerce revenue is expected to reach USD 136 billion this year[4]. Livestream shopping (known as live commerce) has become very popular especially during the Covid-19 pandemic, as the retail industry finds innovative ways to generate revenue and seeks to minimise the losses suffered by their "bricks and mortar" stores. Key opinion leaders have been driving live commerce transactions by livestreaming themselves trying retail

3 Reported by China's Ministry of Commerce.
4 Reported by iiMedia Research.

products and providing comments to viewers. Viewers can often ask questions in real-time, and seek information about products and how to buy them.

The success of live commerce has been dampened by concerns of false and misleading advertising and poor customer service. As a result, the CAA has ramped up its efforts to regulate the sector and has issued the Code of Conduct, urging content censorship and real name user registration.

Who is Subject to the Code of Conduct?

The Code of Conduct applies to merchants, livestreamers and livestreaming platforms.

Definitions	
Merchants	Business entities that sell goods or provide services in livestreaming marketing activities (e.g. retailers and brand owners).
Livestreamers	Individuals that directly interact with users in livestreaming marketing activities (e.g. key opinion leaders).
Livestreaming platforms	Platforms that provide livestreaming technical services for livestreaming marketing activities, including e-commerce platforms, content platforms, and social media platforms.

What Does the Code of Conduct Require?

The Code of Conduct requires merchants to provide the livestreaming platform with evidence of their incorporation and their ownership or right to use the relevant brand being promoted (e.g. business licence, trade mark registration certificate, etc.). Merchants must also ensure that the goods or services being marketed are compliant with PRC laws and regulations, including law and regulations pertaining to quality and safety requirements, and that they do not infringe the rights of any third party.

Livestreamers are required to create a user account with the livestreaming platform using their actual legal name and to provide identification credentials for verification. They cannot allow any third party to use their account, nor can they falsify any data used for marketing purposes (such as sales figures and viewership data), or use obscene, vulgar, risky, absurd, offensive, slanderous language or language that can be seen as insulting, harassing or unethical during livestreaming sessions. The promotion or advertising of tobacco products is banned. This includes a prohibition on smoking during a livestreaming session.

Neither merchants or livestreamers are allowed to convey any false or misleading messages meant to to deceive and mislead consumers about the relevant goods and services being promoted via the live streaming session.

Lastly, livestreaming platforms are responsible for taking action against prohibited online marketing activities and implementing rules that safeguard consumers and intellectual property rights. This includes establishing an effective mechanism for handling complaints and responding to any marketing activities that are illegal or breach the Code of Conduct.

How is the Code of Conduct Enforced?

Whilst the Code of Conduct does not carry the force of law, any violations may result in warnings, rectification orders, ongoing supervision or public naming-and-shaming by the CAA. In addition, if there is a suspected breach of any laws or regulations, the CAA may refer the matter to the relevant government authorities for further investigation and handling.

Conclusion

Currently, there are no laws in China that specifically target live streaming marketing activities, leaving this flourishing industry largely unregulated, save to the extent that China's Advertising Law and other general regulations may apply. The lack of supervision has magnified issues bubbling under the surface, and the introduction of the Code of Conduct undoubtedly signals the government's intention to crack down on dishonest marketing practices, and heralds stricter regulations in the future.

*The authors would like to thank **Sophie Huang**, Intellectual Property Officer at Mayer Brown, for her assistance with research for this article.*

A New Era of Paperless Proceedings in Hong Kong

By **Amita Haylock, Partner**
Mayer Brown, Hong Kong

Jacqueline W. Y. Tsang, Associate
Mayer Brown, Hong Kong

Hong Kong has been lagging behind other common law jurisdictions in the use of technology in its courts. However, recent developments in legislation and case law demonstrate the commitment of Hong Kong's Judiciary to switch to paperless electronic proceedings.

Enactment of the Court Proceedings (Electronic Technology) Ordinance

On 17 July 2020, the Court Proceedings (Electronic Technology) Ordinance (Cap.638) (the "**Ordinance**") made its way through the Legislative Council's second and third readings. While the Ordinance has yet to come into effect, it provides for the use of electronic technology ("**e-technology**") in court proceedings as an alternative to conventional paper-based proceedings.[5]

The enactment of the Ordinance is part of the Judiciary's *Information Technology Strategy Plan*, which aims to gradually implement a streamlined and standardised court process with the assistance of information technology.[6] The Judiciary has been developing an integrated court case

5 Explanatory Memorandum of the Court Proceedings (Electronic Technology) Bill (the "**Bill**"), paragraph 1

6 *Judiciary Administration's work in implementing projects under Information Technology Strategy Plan*, Audit Commission (28 October 2019).

management system (iCMS) to facilitate the use of e-technology in court proceedings. This system is expected to be implemented in phases, first in the District Court and part of the Magistrates' Courts.[7]

When in force, the Ordinance will introduce the following uses of e-technology in designated proceedings[8]:

- Documents created, issued or sent by, or sent to the courts in writing may be electronically submitted through iCMS[9]
- Documents in writing may be electronically served between parties[10]
- Authentication (e.g. signature, sealing and certification) of documents sent to court, or served by or on parties can be done electronically, including using digital signature and electronic signature[11]
- An original or certified document can be sent to a court by sending its electronic copy[12]
- A document can be conveyed or produced to the court by sending its electronic copy[13]
- Printouts of electronic documents issued or sent by courts have the same legal effect as the original document or a copy of it[14]
- A document, file or record can be kept, maintained or made in electronic form for an e-proceeding in an e-court[15]

The Ordinance further makes it clear that an act done electronically according to the Ordinance will have the same effect as an act done using a paper document.[16] The fees payable in respect of a court-related matter that is carried out via an electronic mode ("**e-fees**") will be determined by the Chief Justice.[17]

Conclusion

Electronic filing already exists in a number of common law jurisdictions, including Singapore (since 2000) and England and Wales (in selected courts such as the Chancery Division since 2015). With the enactment of the Ordinance and the Judiciary's increasingly technology-friendly attitude, Hong Kong will find itself more in line with other common law jurisdictions on the implementation of technology in proceedings.

Although the Ordinance is yet to come into force, and the applicable rules and practice directions remain to be seen, the Hong Kong legal profession welcomes the proposed changes as a major step to incorporate information technology in court proceedings. As Coleman J noted in the recent case *Hwang Joon Sang v Golden Electronics Inc.*[18], making use of technology and going paperless reduces both the financial and time costs involved in court proceedings. This promotes fairness and improves access to justice to less affluent litigants. Furthermore, e- technology benefits the environment by significantly reducing paper generation and usage.

*The authors would like to thank **Keith So**,* Seconded Trainee at Mayer Brown, for his assistance with research for this article.

7 Press Release, *Court Proceedings (Electronic Technology) Bill gazetted* (Hong Kong Government Press Release, 27 December 2019).
8 Such use will be subject to rules and practice directions (also known as "**e-rules**" and "**e-practice directions**") to be issued by the Chief Justice: see sections 26-27 of the Ordinance.
9 Sections 13-15 of the Ordinance
10 Section 16 of the Ordinance
11 Sections 17-19 of the Ordinance; Second Reading of the Bill
12 Section 20 of the Ordinance
13 Section 21 of the Ordinance Section 22 of the Ordinance
14 Section 22 of the Ordinance
15 Section 23 of the Ordinance
16 Section 25 of the Ordinance
17 Sections 28-31 of the Ordinance
18 Hwang Joon Sang and another v Golden Electronics Inc. and others [2020] HKCFI 1223 - a recent case where the court permitted service of documents via an online data room.

International Trade Mark Registrations - Hong Kong Takes First Step in Implementation of Madrid Protocol

By **Michelle G. W. Yee, Counsel**
Mayer Brown, Hong Kong

Introduction

After years of anticipation, Hong Kong has finally taken the first step in the implementation process for the Protocol ("**Madrid Protocol**") relating to the Madrid Agreement Concerning the International Registration of Marks ("**Madrid Agreement**"). The Trade Marks (Amendment) Ordinance 2020 ("**Amendment Ordinance**"), which was gazetted and took effect on 19 June 2020, introduces new provisions relating to the implementation of the Madrid Protocol in Hong Kong, including empowering the Trade Marks Registrar to devise the relevant procedural rules and amending existing Trade Marks Ordinance ("**TMO**") provisions to include references to international registrations. Separately, the Amendment Ordinance also makes certain technical amendments to the TMO and enhances the enforcement powers of the Customs and Excise Department by making it the sole enforcement authority responsible for dealing with trade mark infringement offences in Hong Kong.

What is the Madrid Protocol?

The Madrid Protocol and the Madrid Agreement are two international treaties that govern the Madrid System for the International Registration of Marks ("**Madrid System**") administered by the World Intellectual Property Organization ("**WIPO**"). The Madrid System provides brand owners from member states with a "one stop shop" to register their trade marks in other member states – instead of filing separate national applications, a brand owner who has filed a mark in their home jurisdiction (called the 'basic application/registration") can use it as the basis to submit an international application through WIPO (in one language and paying one set of fees) designating one or more other member states. WIPO will coordinate the requests with the IP office of each designated member state, eliminating the need for the brand owner to deal directly with the local IP offices in different local languages and having to pay separate sets of official fees in different currencies.

What Will it Mean for Hong Kong?

Although China is a contracting party to both the Madrid Protocol and the Madrid Agreement, Hong Kong, which is considered a separate jurisdiction for trade marks, has not been part of the Madrid System. Currently, foreign brand owners looking to register their mark in Hong Kong must file a separate application directly with the Hong Kong Trade Marks Registry, and Hong Kong brand owners expanding into the global market must either file an international application through an affiliate located in a Madrid member state or deal with the cumbersome administrative work of filing separate national applications in each market. The implementation of the Madrid Protocol in Hong Kong will allow both foreign and local brand owners to benefit from the efficiencies of the international registration system.

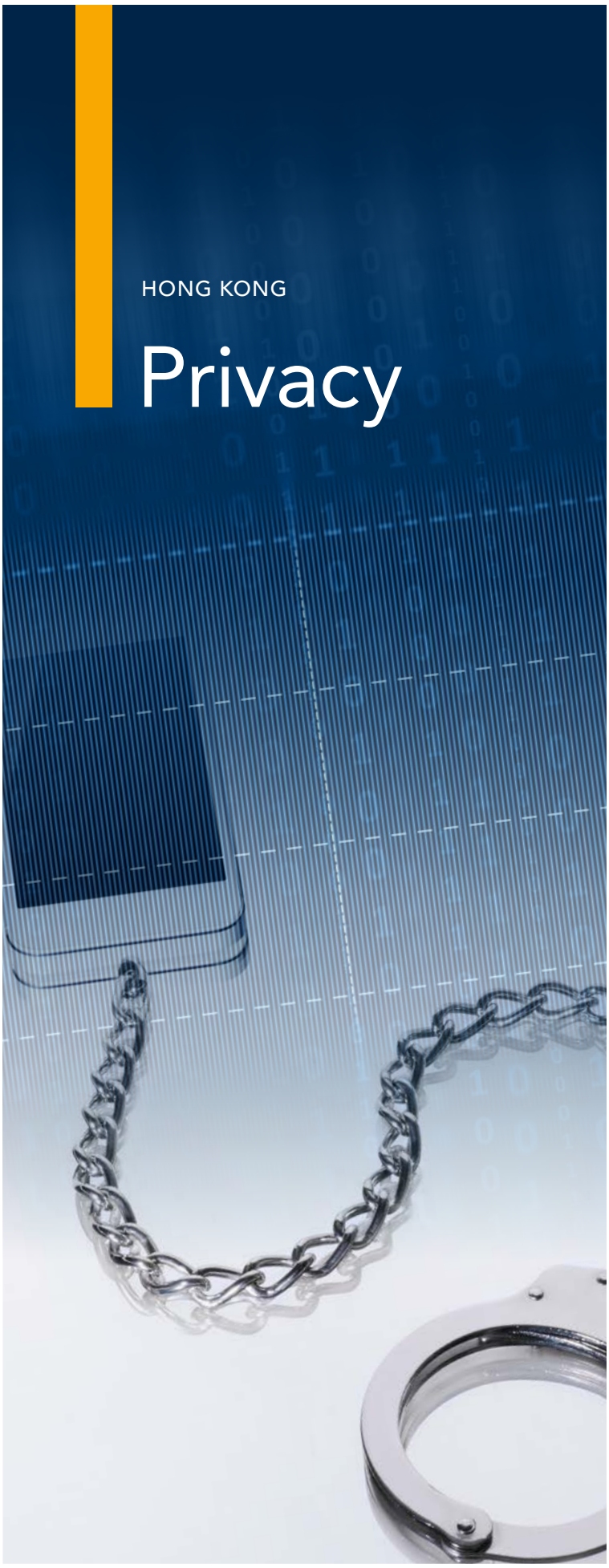
What's Next?

Further steps will now be taken to prepare for full implementation of the Madrid Protocol in Hong Kong, including formulating relevant procedural rules for international registrations and putting in place the necessary IT systems and workflows required to process applications filed through the Madrid System. The Trade Marks Registrar has indicated that the current plan is to implement the international registration system in Hong Kong in 2022 or 2023 at the earliest.

Is an International Registration Right for You?

Whilst the Madrid System offers a number of important advantages for brand owners seeking to expand protection of their marks internationally, an international registration may not be the most appropriate solution in every instance. For example, brand owners will only significantly benefit from the cost and administrative efficiencies afforded by the Madrid System if they designate a relatively large number of jurisdictions – an international registration may not be appropriate for marks that are only used in specific markets, such as local language marks. Marks filed through the international system are also uniquely vulnerable to a so called "central attack" for the first five years, during which the validity of protection in the designated member states will depend on the validity of the basic application/registration in the applicant's home jurisdiction. This means that if a third party successfully challenges a brand owner's basic application / registration, the extension of protection to other jurisdictions through the corresponding international registration will no longer be valid. Hong Kong brand owners also need to be aware that, because the Madrid Protocol is an international treaty among nation states, it would not be possible for a Hong Kong applicant to designate China through an international registration (and vice versa), although there are ongoing discussions between relevant authorities in Hong Kong and Mainland China on possible administrative measures to address this issue. These and other factors, such as timing for launch of the brand in different markets, should be carefully considered before deciding whether to proceed with an international registration.

*The authors would like to thank **Sophie Huang**, Intellectual Property Officer at Mayer Brown, for her assistance with research for this article.*



Peek-a-Boo I've Caught You – New Offences Against Upskirt Photos and Blackmail

By **Karen H. F. Lee, Counsel**
Mayer Brown, Singapore

In July 2020, the Hong Kong Security Bureau issued a consultation paper for the proposed introduction of first-ever offences against voyeurism, intimate prying, non-consensual photography of intimate parts, and the distribution of related images ("**Proposal**").

Background

The use of smartphones to take upskirt photos and other intimate images without consent have long been an issue of concern. However, whilst reprehensible, such acts do not amount to a direct offence under Hong Kong law. Instead, prosecutors have had to charge wrongdoers under other loosely related offences, including breach of the Personal Data (Privacy) Ordinance ("**PDPO**"), the offence of outraging public decency, disorder in public places, loitering and access to a computer with criminal or dishonest intent. Most of these charges often attract relatively light punishments, which are not commensurate with the severity of voyeurism and clandestine intimate photography.

In particular, charging wrongdoers with the offence of access to a computer with criminal or dishonest intent has been accused of being used as a "one-size-fits-all" offence to prosecute any

smartphone-related act. In April 2019, the Court of Final Appeal upheld a decision that the offence of obtaining access to a computer with criminal or dishonest intent cannot apply to a person using their own smartphone or computer. Therefore, a person who uses their own phone to take upskirt photos or distribute related images cannot be charged with such an offence. This decision has further limited the prosecutors' ability to combat voyeurism-related acts, resulting in calls in the city for specific offences and criminal sanctions.

With regard to data privacy, unlike other jurisdictions (such as France, the UK and New Zealand), Hong Kong does not grant a statutory or common law actionable right to privacy. The Basic Law and Bill of Rights of Hong Kong protect a person's right to freedom and privacy of communication and from arbitrary or unlawful interference with their privacy, whilst the PDPO provides protection in relation to the handling of personal data regarding an individual (i.e. data from which it is practicable to identify the individual, directly or indirectly). However, Hong Kong's laws do not recognise a general tort of invasion of privacy – a person would have to argue that their privacy was intruded upon by means of private nuisance, breach of confidence, trespass to land, or their data privacy rights have been breached under the PDPO.

Celebrities in particular have relied on the PDPO to file complaints in relation to the capturing of photos of them in their private homes by journalists, which were found to be an unfair collection of personal data. People who distribute videos or photographs of victims as part of revenge porn or for other reasons (e.g. blackmail, sale for profit, etc.) might also be guilty of an offence under Section 64 of the PDPO, which criminalises the disclosure of personal data taken from a data user, without their consent, with the intent to obtain a gain or cause a loss to the victim, or which otherwise causes psychological harm to the victim. This can incur a maximum fine of HK$1,000,000 and 5 years' imprisonment. The PDPO remains limited in its ability to assist victims of revenge porn or acts of voyeurism. If there is any live streaming (i.e. no actual recording or capturing of data), the victim cannot be identified (directly or indirectly), and/or the wrongdoer is not trying to "collect" data regarding the victim (i.e. they are not seeking to identify the victim, as they only wish to sell their intimate images or videos to third parties for profit) then the PDPO will not apply.

The Proposal is an attempt to plug the glaring whole in the legislation.

Offences of Voyeurism and Intimate Prying

The Proposal seeks to introduce the new offence of voyeurism and intimate prying. Voyeurism amounts to observing or recoding any intimate act for the purpose of obtaining sexual gratification. In comparison, intimate prying involves observing or recording any intimate acts, irrespective of the purpose (i.e. whether or not it is for sexual gratification), without the victim's consent, and regardless of whether any equipment is used in aid of such conduct. This could cover instances such as revenge porn, blackmail or the recording and sale of private photos or videos for profit. The offence of intimate prying, in addition to being a standalone offence, would also act as a statutory alternative to voyeurism in case prosecutors are unable to prove sexual motives.

An intimate act is defined as any act committed by a person in a place which would reasonably be expected to provide privacy, and which exposes "intimate parts" or involves certain private conduct.

Installing equipment or constructing or adapting a structure or part of a structure with the aim of enabling a person to commit either offence also falls within the scope of these proposals.

Offences of Non-Consensual Photography

The Proposal also seeks to introduce the offence of non-consensual photography of intimate parts in order to tackle upskirt photography. Anyone who, without the consent of the victim, operates equipment beneath the clothing of the victim to enable the person or another person to observe the victim's intimate parts or record related images (including stills and videos) or to have access to such recorded images, in circumstances where the intimate parts would not otherwise be visible, commits an offence. There are two separate offences, one involves the taking of intimate photos for the purpose of sexual gratification, whereas the other applies regardless of motive. Whether such acts are committed in public or private place is immaterial. "Intimate parts" would be defined as a

person's genitals, buttocks or breasts, whether exposed or covered only with underwear.

Offences of Distribution of Surreptitious Intimate Images and Non-Consensual Distribution of Intimate Images

There is currently no specific law that criminalises the publishing, circulation, selling or distribution of videos or photographs taken in relation to upskirt photos, or which were originally taken with the consent of the victim (e.g. by a partner) and then circulated for blackmail or revenge purposes (commonly known as revenge porn). At most, prosecutors may be able to rely on the Control of Obscene and Indecent Articles Ordinance which concerns the public dissemination of obscene and indecent materials, but is insufficient to cover situations where intimate videos or photos are circulated amongst a select group of people.

The Proposal therefore seeks to introduce a specific offence against the distribution by any means of images (including still and videos), known to have been obtained from voyeurism, intimate prying or non-consensual photography of imitate parts, for whatever purpose.

A separate offence of non-consensual distribution of intimate images also aims to protect the victim in cases where consent might have been given to the taking of such images (e.g. intimate images or videos taken by or with the victim's consent in private), but not to the subsequent distribution.

Defences

It is suggested that a defence of lawful authority or reasonable excuse, similar to the statutory defences provided in other jurisdictions, should be made available for some of the proposed offences. For example, intimate images taken or distributed for the purposes of journalistic work; for genuine scientific, educational or medical purposes; or if reasonably necessary for the purpose of legal proceedings.

Sexual Conviction Record Check Scheme

Some of the new offences may be listed as part of the Specific List of Sexual Offences under the Sexual Conviction Record Check Scheme. The Sexual Conviction Record Check Scheme allows employers to ascertain whether potential employees who will be working with children or mentally incapacitated persons have any criminal conviction records against a specified list of sexual offences.

Conclusion

Members of the public have until early October 2020 to submit their views on the Proposal. The rapid development of technology over the last couple of decades has given rise to a stream of new types of reprehensible conduct ranging from revenge porn and upskirt photographs, to doxing and cyberbullying. The Proposal is a step in the right direction, and has been a long time coming. However, further changes in the law need to be made to keep pace with the digital age.

*The author would like to thank **Sophie Huang**, Intellectual Property Officer at Mayer Brown, for her assistance with research for this article.*

Contact Us

Gabriela Kennedy
Partner
+852 2843 2380
gabriela.kennedy
@mayerbrown.com

Amita Haylock
Partner
+852 2843 2579
amita.haylock
@mayerbrown.com

Karen H. F. Lee
Counsel
+65 6327 0638
karen.hf.lee
@mayerbrown.com

Michelle G. W. Yee
Counsel
+852 2843 2246
michelle.yee
@mayerbrown.com

Cheng Hau Yeo
Associate
+65 6327 0254
chenghau.yeo
@mayerbrown.com

Jacqueline W. Y. Tsang
Associate
+852 2843 4554
jacqueline.tsang
@mayerbrown.com