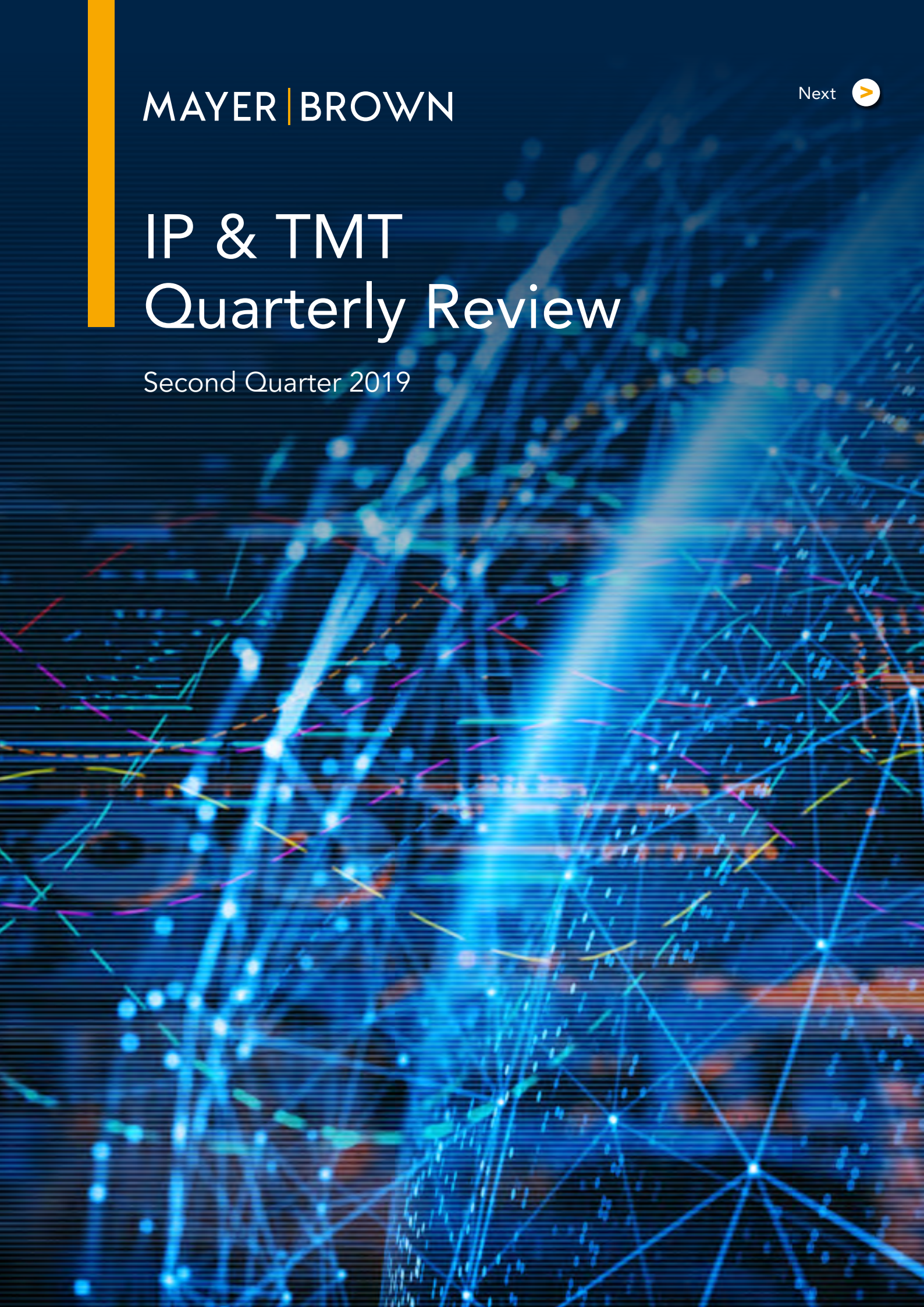
MAYER | BROWN

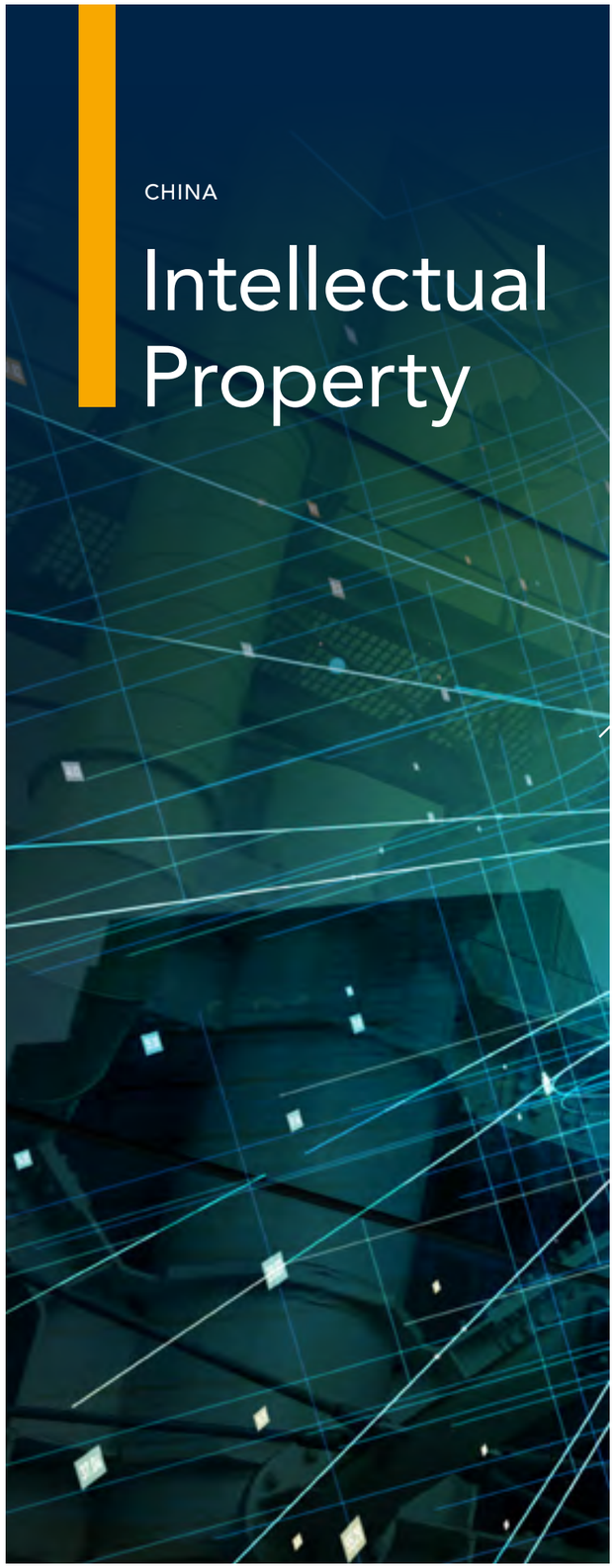
Next

IP & TMT Quarterly Review

Second Quarter 2019



Contents



Winning Strategies for Chinese Patent Owners and Challengers in U.S. Pharmaceutical Patent Disputes

By Gary Hnath, Partner
Mayer Brown, Washington DC

Lisa Ferri, Partner
Mayer Brown, New York

Jing Zhang, Associate
Mayer Brown, Washington DC

Scott McMurry, Associate
Mayer Brown, New York

Elliot Choi, Associate
Mayer Brown, New York

Introduction

In the United States, the majority of disputes involving pharmaceutical patents are resolved through one of two processes – post-grant proceedings at the United States Patent and Trademark Office ("**USPTO**"), or litigation under the "Hatch-Waxman Act" in a United States District Court. Understanding the details of these processes is key to choosing the right forum to resolve disputes over pharmaceutical patents in the United States. This article summarizes the advantages and disadvantages of these processes for Chinese pharmaceutical companies looking for the best strategy to enter the U.S. market.

Post-Grant Proceedings

The Leahy-Smith America Invents Act ("**AIA**"), enacted in 2012, established post-grant proceedings before the Patent Trial and Appeal Board ("**PTAB**") of the USPTO to be streamlined mechanisms to challenge the validity of U.S. patents. These proceedings involve mini-trials between the patent challenger ("**the Petitioner**") and the patent owner. The proceedings are conducted before three or more Administrative Patent Judges who are well versed in the technology, law, and procedures involved in determining the validity of a patent.

The AIA established two types of post-grant proceedings which are relevant here — **Inter Partes Review** and **Post-Grant Review**.

1. INTER PARTES REVIEWS ("IPR")

(a) Who can file an IPR?

Any person other than the owner of a challenged patent can file an IPR petition to challenge the validity of a U.S. patent. However, the petitioner cannot have previously filed a civil action in a U.S. court against the same patent. Each party to the IPR must be represented by a registered U.S. patent attorney or patent agent, and lead and backup counsel must be identified for each party. Since 2012, when IPRs became available, the number of petitions filed has increased dramatically each year and IPRs have become a very popular procedure for companies wishing to invalidate U.S. patents.

Figure 1. Litigation & IPR Trends

(b) When can an IPR be brought?

An IPR petition cannot be filed until nine months after patent issuance and after the termination of any Post-Grant Review ("**PGR**") challenge. Furthermore, a petitioner must file its IPR petition within one year of being served with a complaint from a district court litigation on the patent at issue, if such a litigation exists. Parties can sometimes join an existing IPR.

(c) How long does an IPR take?

The PTAB must complete an IPR within twelve months of institution, although it can extend that deadline for an additional six months, but only for "good cause," which is rarely found.

(d) On what grounds can an IPR be brought?

Patents in an IPR can be challenged only on § 102 (Novelty) and § 103 (Obviousness) grounds, using only published prior art (patents and printed publications). To institute an IPR, the petition must establish a reasonable likelihood that at least one of the challenged claims is invalid.

(e) Who has the burden of proof?

The petitioner bears the burden of proving unpatentability by a preponderance of the evidence, because no presumption of validity exists for a patent challenged in an IPR.

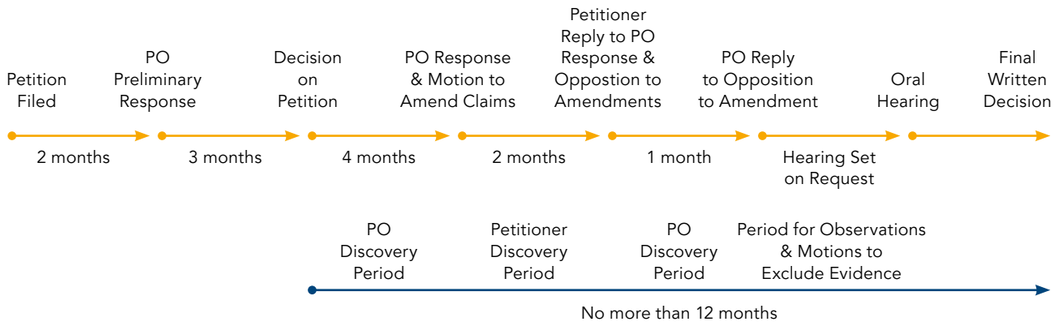
(f) Claim Construction:

For IPRs filed before 13 November 2018, the PTAB gives claim terms their broadest reasonable interpretation unless the challenged patent expires before or during the IPR, in which case the claims are given their ordinary and customary meaning. For IPRs filed on or after 13 November 2018, the PTAB gives claim terms their ordinary and customary meaning consistent with the claim construction standard used in federal district court.

(g) Timeline for an IPR:

The timeline for an IPR is shown below. Note that each filing has strict limitations on length.

Figure 2. Timeline of an IPR.



The first step in an IPR is filing a petition by the party challenging the patent. The petition must explain in detail how the prior art renders the claims anticipated or obvious, must construe any necessary claim terms, and should be supported by a declaration from an independent expert. Once the PTAB determines that all papers are in order, it assigns the petition a filing date from which all remaining deadlines are calculated.

Within three months after the PTAB accepts the petition, the patent owner can and should file a patent owner preliminary response ("**POPR**"). The POPR should point out any factual or legal gaps in the petition, present evidence in support of validity, and construe any necessary claim terms. The patent owner may file an expert or other declaration to support its argument.

Within six months after the petition is filed, the PTAB will issue a decision on whether an IPR should be instituted. To institute, the PTAB must find that the petition has raised a reasonable likelihood that at least one of the challenged claims is invalid. In that case, the PTAB will institute the IPR on all challenged claims and on all grounds raised in the petition. If the institution is denied on all challenged claims, the IPR is terminated and the patent remains valid. On the date of institution, the PTAB will issue a scheduling order specifying all future deadlines, including the times for conducting routine discovery.

Within three months after the institution decision (approximately nine months after the petition's filing date), the patent owner must file its patent owner response ("**POR**"). The patent owner may also submit an amendment of its claims to try to avoid the prior art. Within three months after the POR is filed, the petitioner must submit a reply that responds to the patent owner's arguments. If the patent owner filed an amendment to the claims, the petitioner must prove why the amended claims are not patentable. Within one month after the petitioner's opposition to the claim amendments, the patent owner may file a reply to the petitioner's opposition.

After the written submissions are completed, an oral hearing before a panel of three Administrative Patent Judges ("**APJs**") is conducted. The USPTO then issues a decision within 12 months of the institution date, or no more than 16 months after the original filing of the challenger's petition.

2. POST-GRANT REVIEW ("**PGR**")

Similar to IPRs, any person other than the patent owner may challenge a patent by filing a petition for PGR. However, PGRs are limited to patents that have an effective filing date of 16 March, 2013 or later. Furthermore, the PGR petition must be filed within nine months of the patent issuance. A PGR petitioner can challenge the validity of a patent claim on any grounds, including prior public use, on-sale activity or public disclosures; or lack of written description, enablement, or patent eligibility.

Once the petition is instituted, the timeline and procedural considerations for PGRs are the same as those for IPRs.

3. SIMILARITIES BETWEEN IPRS & PGRS

IPRs and PGRs combine features of patent prosecution and litigation. Similar to prosecution, no presumption of validity applies to the challenged patent, and the burden of proof is a preponderance of the evidence. For IPRs and PGRs filed before 13 November, 2018, claim terms are construed according to their broadest reasonable interpretation (except in the limited circumstances explained in Section II.A.). For IPRs and PGRs filed on or after 13 November, 2018, claim terms are construed according to their ordinary and customary meaning, consistent with the claim construction standard used in federal district court. IPRs and PGRs allow very limited discovery. All information relied on in any filing must be disclosed to the PTAB and to the other party, or it will not be considered. Confidential information can be sealed from public disclosure with the PTAB's permission. Additional discovery is allowed if the parties agree to it or if the PTAB finds it to be in the interests of justice, and as noted above is generally very limited. A disadvantage to IPRs and PGRs for the challenger is that a final written decision creates estoppel that prohibits the challenger from later raising in a district court litigation the same grounds or grounds that could have been raised in the IPR or PGR.

4. DIFFERENCES BETWEEN IPRS & PGRS

The following table summarizes some of the key differences between an IPR and a PGR.

	Institution Standard	Grounds	Timing
PGR	More likely than not invalid OR Important novel or unsettled legal question	35 U.S.C. § 101, § 102, § 103, § 112 (but not best mode), double patenting	Up to 9 months after patent grant or reissue
IPR	Reasonable likelihood of invalidity (lower institution standard than for PGRs)	35 U.S.C. § 102 and § 103, based only on patents and printed publications	For first-inventor-to-file: after the later of (i) 9 months after patent grant or reissue, or (ii) the termination of any post-grant review of the patent For first-to-invent (pre-AIA): any time after grant or reissue, except for petitions (i) filed more than one year after being sued for infringing the patent, or (ii) after petitioner filed a lawsuit on the patent

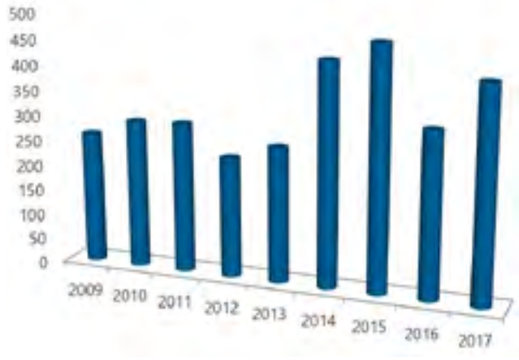
As noted in the chart above, in IPRs, only challenges under 35 U.S.C. §102 and §103 and based on printed publications are allowed. In contrast, PGR challenges to a patent can be based on any statutory defense to infringement, including anticipation, obviousness, ineligible subject matter, indefiniteness, lack of enablement, or lack of written description. These last two defenses can be particularly meaningful in the context of pharmaceutical patents. Because the development of pharmaceuticals is unpredictable, patents in the pharmaceutical field often need to disclose more information or examples of the invention claimed than patents in more predictable fields to meet these two requirements.

Thus, the IPR and PGR procedures offer Chinese pharmaceutical companies a relatively fast and effective means for canceling patents that might otherwise serve as a barrier to entry into the U.S. market.

Hatch-Waxman District Court Litigation

A second alternative available to Chinese pharmaceutical companies is the procedure described in the Drug Price Competition and Patent Term Restoration Act of 1984, commonly known as the "Hatch-Waxman Act." This Act attempts to strike a balance between encouraging the development of pioneer pharmaceutical treatments and introducing lower cost generic drugs. To achieve these goals, the Hatch-Waxman Act grants branded pharmaceutical companies an extension of patent term to make up for delays from the U.S. Food and Drug Administration's ("**FDA**") approval process and automatically stays the entry of a generic drug for thirty months from the date a patent infringement lawsuit is commenced under the Act. The Hatch-Waxman Act also allows generic drug companies to develop their generic products free from the threat of a patent infringement lawsuit as the product is being developed and tested. As an added incentive to bring generic drugs to the market, 180-day marketing exclusivity is also granted to the first generic drug company to successfully challenge the patents covering a branded drug. Due to these incentives, district court litigations under the Hatch-Waxman Act have become a popular avenue for resolving pharmaceutical patent disputes.

Figure 3. District Court Filings Under the Hatch-Waxman Act



Under the Hatch-Waxman Act, branded companies must list with the FDA any patents that cover the drug or an FDA-approved method of using the drug in the "Orange Book" (Approved Drug Products with Therapeutic Equivalence Evaluations).

Figure 4. The Orange Book

If the new drug contains an active ingredient that has never before been approved by the FDA, five years of data exclusivity (New Chemical Entity Exclusivity) are granted to the New Drug Application ("**NDA**") holder from the date of approval. This data exclusivity prevents a generic drug company from seeking approval of a generic version of the drug until five years after the first approval of the branded version.

To obtain approval to market a generic copy of a branded drug, generic drug companies file an Abbreviated New Drug Application ("**ANDA**") with the FDA. For each patent listed in the Orange Book, generic drug companies must certify one of the following in the ANDA application:

i. Paragraph I: No patent is listed,
ii. Paragraph II: The listed patents have expired,
iii. Paragraph III: The listed patent, plus any other exclusivity, will expire before the generic version would be approved, or
iv. Paragraph IV: The patent is invalid or will not be infringed by the manufacture, use, or sale of the generic version of the drug.

With a Paragraph IV certification against a drug having New Chemical Entity Exclusivity, a generic drug company can file their ANDA one year before the New Chemical Entity Exclusivity expires.

The filing of an ANDA containing a Paragraph IV certification is considered a technical act of infringement and allows the filing of a lawsuit for patent infringement. The ANDA applicant must notify both the NDA holder and the patent owner within twenty days of the FDA's acceptance of the ANDA. In its Paragraph IV certification, the ANDA applicant must provide the full, detailed factual and legal bases for its Paragraph IV certification that the patent or patents are invalid and not infringed. Furthermore, any allegation of non-infringement must be accompanied by an offer for confidential access to the ANDA to allow the patent owner to determine whether the patent is infringed. After receiving the notice of the Paragraph IV certification, the branded company has 45 days to file suit for patent infringement. Once the lawsuit is filed, a thirty-month stay of FDA approval of the generic version of the drug is triggered. If no lawsuit is filed, the thirty-month stay is forfeited and the FDA can immediately approve the generic version.

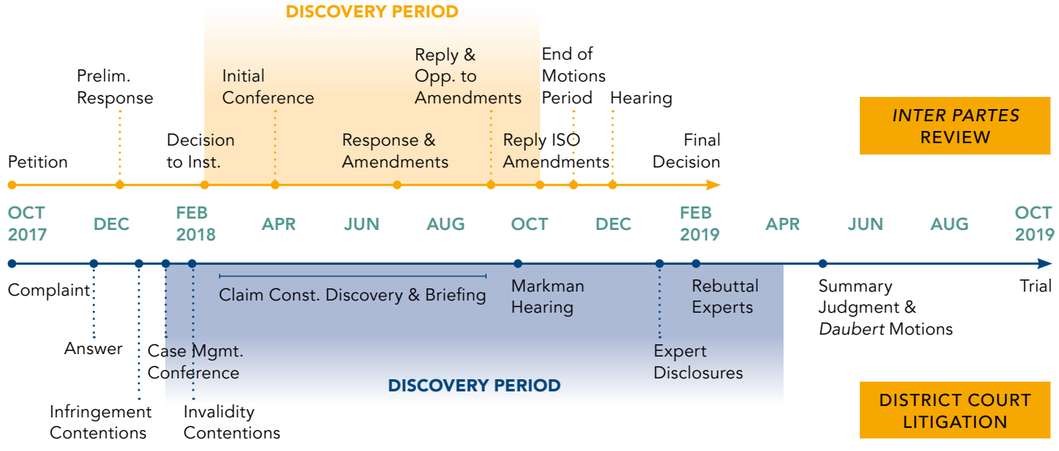
Winning Strategies for Chinese Pharmaceutical Patent Owners and Challengers

Due to the extremely fast-moving nature of IPRs and PGRs, it is imperative that Chinese patent owners perform due diligence on their patents as soon as possible. Patent owners have no control over when an IPR will be filed, and waiting until one is filed often means that it is too late to develop a full case to preserve the validity of the patent, including, for instance, evidence of commercial success. Evidence of unexpected results can win the day for patent owners, but developing convincing evidence often takes time. Therefore, because of the fast-moving nature of IPRs and PGRs, pharmaceutical patent owners should start preparing a validity case to protect their key patents as soon as they issue.

District court litigations asserting patent infringement under the Hatch-Waxman Act provide the benefit of an automatic thirty-month stay of FDA approval of the generic drug and far more time to investigate and develop a validity case to protect a patent, particularly for unexpected results, which can win the day. However, whether a patent challenger chooses the IPR/PGR or the Hatch-Waxman route is out of the patent owner's control.

Chinese pharmaceutical companies wishing to enter the market should consider their options for challenging U.S. patents, such as those listed in the Orange Book, that can block approval of a generic version of a drug. Procedurally, IPRs and PGRs are faster than Hatch-Waxman district court litigations, with final decisions rendered within 12 months after institution. Substantively, IPRs and PGRs have a lower burden of proof than district court litigations, because they do not presume that the challenged patent is valid. Furthermore, PTAB judges are generally very knowledgeable about the technologies and U.S. patent law and procedures. Therefore, if a challenger has a strong invalidity argument, the IPR/PGR option may be preferable.

Figure 5. An Example of a Timeline of an IPR, a PGR, and a District Court Litigation.



While IPRs and PGRs can be a powerful tool for generic companies, they have certain limitations. For instance, the first generic company to successfully challenge an Orange book patent when filing an ANDA will receive 180 days of market exclusivity, which is not available through an IPR or PGR. If this exclusivity is important, the Hatch-Waxman option may be preferred. In addition, district court litigations have no restrictions on the grounds, including non-infringement, that can be raised and provide much more time for each party to develop its case.

Chinese companies can proactively monitor the progress of patent applications and file PGRs promptly after issuance. U.S. patent applications are published eighteen months after their earliest filing date, and take an average of 20 to 30 months to issue. Patent counsel can assist with this monitoring process. PGRs can then be filed immediately after a patent issues and are a fast and powerful way to defuse blocking patents if a challenger has strong evidence that a patent is invalid.

Conclusion

Chinese pharmaceutical companies have a number of tools at their disposal to protect their intellectual property rights, if they are U.S. patent holders, or to invalidate patents that could serve as a barrier to their entry into the U.S. market. Chinese companies that are unfamiliar with the intricacies of U.S. pharmaceutical patent law, however, can inadvertently lose patent protection on their products or be found to infringe U.S. patents. Chinese pharmaceutical companies therefore should consult with experienced U.S. patent attorneys who are intimately familiar with pharmaceutical patent disputes in the U.S. over how to choose the best strategy to effectively compete in the U.S. market.

Trade Mark Hijackers Beware – New Measures to Target Bad Faith Applications

By Gabriela Kennedy, Partner
Mayer Brown, Hong Kong

Michelle G.W. Yee, Senior Associate
Mayer Brown, Hong Kong

Introduction

The revised Trade Mark Law was enacted in 2014 to much fanfare, as it included important new provisions targeting bad faith applications by trade mark hijackers, a recurring problem that has plagued brand owners in China. Unfortunately, in the 5 years since the enactment, the new provisions have done little to reduce trade mark hijacking activity and the onus has remained with brand owners to oppose or invalidate hijacked marks.

Recently, the Chinese Government has signalled its renewed efforts to target bad faith applications through a series of regulations and amendments to the Trade Mark Law. In February 2019, the National Intellectual Property Administration of China ("**CNIPA**") published 'Several Measures on Regulating Trade Mark Filing for Registration (Draft for Comment)' ("**Draft Regulations**") for public consultation. The consultation period ended on 14 March 2019 and as of the date of writing, the Draft Regulations are still being finalised. Separately, the Standing Committee of the National People's Congress approved amendments to the Trade Mark Law to take effect from 1 November 2019 ("**2019 Amendment**"). Both the Draft Regulations

and the 2019 Amendment aim to address bad faith registration of trade marks in China, in order to prevent trade mark hijackers from exploiting the registration system.

2019 Amendment

The 2019 Amendment provides for the rejection of bad faith applications filed without intent to use (Article 4), and this ground can also be pleaded in opposition (Article 33) or invalidation (Article 44) proceedings. Trade mark agencies are also obligated to reject instructions where they know or should have known that the applications are filed in bad faith without intent to use (Article 19), and those that file bad faith applications will be subject to administrative penalties such as warnings or fines (Article 68). The 2019 Amendment also provides that the courts may impose penalties in relation to trade mark lawsuits filed in bad faith.

Apart from the above provisions targeting bad faith applications, the 2019 Amendment also introduces new measures to target trade mark infringement in Article 63, including: (1) increasing the maximum statutory damages for infringement from RMB 3 million to RMB 5 million; (2) increasing the maximum multiplier for punitive damages for serious and malicious infringement from three to five; (3) empowering the courts to order the destruction of counterfeit goods, and the materials and tools used to manufacture such goods; and (4) prohibiting counterfeit goods from being redistributed in the market, even after the infringing mark has been removed.

Intent to Use – a Double-Edged Sword?

There has been some concern that the "intent to use" requirement introduced by the 2019 Amendment may block legitimate applications filed by brand owners for defensive purposes. This is clearly not the intention of the drafting committee, as the "intent to use" requirement was coupled with bad faith specifically to address this issue (the original wording of the "intent to use" amendment to Article 4 made no reference to bad faith). Nevertheless, there remains a possibility that third parties may try to oppose or invalidate marks filed by brand owners for defensive purposes on the ground that there was no bona fide intention to use.

Another potential issue is that the "intent to use" requirement could, at least in theory, be circumvented by hijackers if they are able to show some use of the mark in question. If implementing regulations are released in the future, they may provide further clarity on the criteria that will be used to determine if an application is filed in bad faith without intent to use.

Draft Regulations – Targeting "Abnormal" Applications

The Draft Regulations also attempt to address trade mark hijacking by targeting "abnormal" trade mark filings, including:

1. applications that copy marks widely recognized by the relevant public and which free-ride on the goodwill of others (Article 3.1);
2. applications for marks that enjoy a "certain degree of influence" and are already being used by others (Article 3.2);
3. applications for similar or identical marks where the applicant knows or should have known of another party's earlier rights (Article 3.3);
4. repeated applications for a clearly improper purpose (Article 3.4);
5. applications filed in large numbers within a short period that clearly exceed reasonable limits (Article 3.5);
6. applications filed without a genuine intent to use, or where there is no actual need to obtain trade mark rights in respect of the relevant goods or services (Article 3.6); and
7. applications that violate the principle of good faith, infringe upon the legitimate interests of other parties, or disrupt the market order (Article 3.7).

Parties who act as trade mark agents or otherwise assist with abnormal filings are also caught by the Draft Regulations (Article 3.8).

Whilst the types of abnormal trade mark filings listed above do cover the more common types of bad faith applications, the definitions are still quite vague. For example, Article 3.5 does not specify the volume of applications that would be considered to exceed reasonable limits – will several dozen applications filed on the same day meet this threshold, or would an applicant need to file hundreds of applications in order to fall within this definition? How will the authorities differentiate between legitimate brand owners with large brand portfolios from trade mark hijackers? Will applications filed by legitimate brand owners for defensive purposes be considered abnormal applications under Article 3.6?

Draft Regulations – Power to Request Explanations and Evidence

The Draft Regulations attempt to curb abnormal filings by empowering the CNIPA to take certain actions against such marks, such as requesting explanations and evidence from applicants of abnormal applications (Article 4.1). However, the Draft Regulations provide no clear guidance on how the CNIPA will determine when explanations and evidence will be necessary – for example, will examiners consult a blacklist, or take the initiative to proactively review an applicant's filing history? The Draft Regulations also provide no clarity on what kind of explanations or evidence will be required, and the timeframes for responding. Without clear guidelines, applicants may find themselves ill-prepared to respond to requests, particularly if they are overseas and are asked to provide extensive use evidence at short notice.

Draft Regulations – Accountability of Trade Mark Agencies

Trade mark agencies that assist with filing abnormal applications will also be held accountable under the Draft Regulations. The Draft Regulations provide for sanctions to be imposed and recorded against an agency's credit file, and for suspension of the agency's licence where there has been a serious breach (Article 4.4). The Draft Regulations also allow the CNIPA to summon agencies that assist with abnormal filings to attend "rectification interviews" (Article 5.4).

Draft Regulations – a Formal Blacklist?

Currently, the CNIPA maintains an informal internal blacklist of bad faith applicants whose applications will automatically be rejected. Whilst brand owners can write to the CNIPA to report bad faith applicants, there is no official procedure or transparency in the current blacklisting process, which is entirely subject to the CNIPA's discretion.

New provisions have been introduced in the Draft Regulations in an attempt to codify the blacklisting process. Article 7 of the Draft Regulations expressly allows any organization or individual to report an abnormal application, and requires for such reports to be dealt with in a timely manner in accordance with the law. Article 5.1 of the Draft Regulations empowers the CNIPA to penalize applicants of abnormal applications by publishing their information on the CNIPA website, which would effectively amount to a formal, publicly accessible blacklist. Nevertheless, the Draft Regulations do not specifically set out a formal blacklisting procedure and much is still left to the CNIPA's discretion. It remains to be seen whether implementing rules or guidelines will be issued to further clarify the process.

In addition to being blacklisted on the CNIPA's website, abnormal filers may also be penalized pursuant to Article 5.1 of the Draft Regulations by having their information entered into the National Credit Information Sharing Platform, which would allow other government departments to impose disciplinary measures.

Conclusion

The introduction of the 2019 Amendment and the Draft Regulations clearly signal the authorities' renewed efforts to target bad faith trade mark applications in China. One lingering concern is whether the new provisions, such as the intent to use requirement under the 2019 Amendment, will have the unintended consequence of blocking applications filed by legitimate brand owners for defensive purposes whilst allowing bad faith applications to proceed as long as the applicant can show some use. Much will depend on how the CNIPA exercises its discretion when applying these new provisions, and it remains to be seen whether these measures will ultimately have the desired effect of curbing bad faith applications.

Hong Kong's Wind of Change – A New Intellectual Property List

By Gabriela Kennedy, Partner
Mayer Brown, Hong Kong

Amita Haylock, Counsel
Mayer Brown, Hong Kong

Introduction

On 6 May 2019, Hong Kong took a significant step up towards enhancing the enforcement of Intellectual Property Rights ("**IPR**") by introducing an IP Specialist List ("**IP List**") in the Court of First Instance of the High Court.

The IP List which is introduced under Practice Direction 22.1 ("**PD 22.1**") aims to facilitate and improve the case management of IP Proceedings (as defined below) in Hong Kong.

A designated Judge (the "**IP Judge**") is in charge of the IP List, and has the power to order the transfer and removal of IP Proceedings. PD 22.1 also provides for the management of interlocutory applications and case management hearings in relation to IP Proceedings, in order to eliminate unnecessary costs and delays. On 6 May 2019 the Chief Justice of Hong Kong appointed the Honourable Mr Justice David Lok as the first IP Judge. The introduction of the IP List is in line with the recommendations and proposals under the Civil Justice Reform of 2009 which aim to streamline civil proceedings in Hong Kong.

Additional changes occasioned by the introduction of the IP List include (1) amendments to existing Practice Direction 11.1 on Ex Parte, Interim and Interlocutory Applications for relief (including Injunctive Relief), which provides that interlocutory applications (including urgent injunctive reliefs) in relation to IP Proceedings will be heard by the IP Judge, Designated Judge or otherwise the Duty Judge; and (2) a revision to the List of High Court Case Types to include a new case prefix, namely "HCIP", in relation to IP Proceedings in the High Court (previously, the case prefix "HCA" was used for IP Proceedings).

Background

Prior to the introduction of the IP List in Hong Kong, IP cases were filed in the General List at the Court of First Instance of the High Court. IP cases were therefore heard before a General List Judge, with no guarantee of subject matter knowledge or experience. This could at times result in a slowing down of the process, a particularly acute issue in IP cases where interlocutory applications (e.g. urgent injunctions) require quick action and orders. The process also suffered from inconsistencies in decisions as interlocutory applications in the same matter could end up being dealt with by different judges in addition to delays and an increase in costs before cases proceeded to trial.

Changes Brought by the Introduction of the IP List Under PD 22.1

1. WHAT ARE IP PROCEEDINGS?

IP Proceedings include: (1) applications, appeals or claims made in respect of trade marks, design, patents, foreign intellectual property, plant variety protection and copyright; (2) claims for passing off; (3) an application made under the Layout-Design (Topography) of Integrated Circuits Ordinance (Cap.445) or a claim made in respect of a protected layout-design (topography); (4) claims which would benefit if the proceedings are commenced or transferred to the IP List, such as claims which involve technical trade secrets, domain names, complicated know-how relating to life science, chemical processes, telecommunications, computer and Internet matters and transactions involving transfer, licensing or restricting the use of IP rights; and (5) contempt proceedings arising from any of these proceedings.

2. ROLE OF THE IP JUDGE

The IP Judge is in control of the actions on the IP List and all interlocutory applications in relation to IP Proceedings. The IP Judge may: (1) make directions and orders regulating the conduct of the trial; (2) issue general directions to improve the regulation of the IP List; and (3) form a consultative committee of legal practitioners for this purpose.

3. HOW TO ENTER THE IP LIST

An applicant who wishes to enter in the IP List needs to mark its originating process document with the words "Intellectual Property List" in a prominent way.

4. HOW TO TRANSFER OR REMOVE PROCEEDINGS FROM THE IP LIST

At any stage of proceedings, the Court may order a transfer to or removal of proceedings from the IP List. This can either be done upon a party's application or upon the Court's discretion.

To apply for a transfer or removal order, a party will first have to seek consent from the other parties in the proceedings. If consent is granted, a party may make an application by letter addressed to the IP Judge, signed by the parties' solicitors, detailing grounds in support of the application and indicating that the application is by way of consent of all the parties. If consent is not granted, the letter addressed to the IP Judge should identify the party that consents to the application and the party that opposes the application.

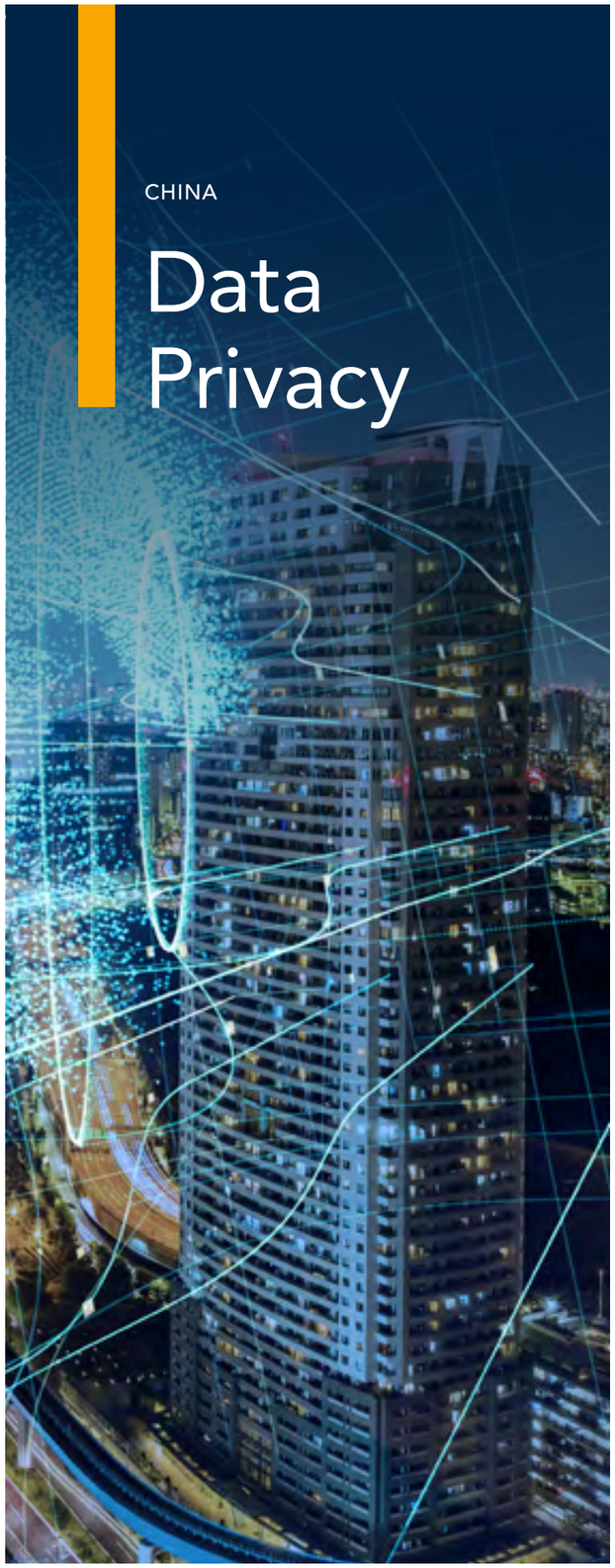
Benefits of a Specialist IP List

An assigned IP Judge who is experienced in IP laws and who is in control of the IP Proceedings will no doubt be able to handle complex IP disputes in a competent and timely manner as well as apply the law consistently.

The introduction of the IP List will bring about improvements to case management. Cases will be managed more effectively from commencement to resolution of proceedings as having only one judge deal with all aspects of a case will inevitably improve the efficiency of proceedings.

Conclusion

It is expected that IP matters will be resolved faster, more competently and with more certainty now that the IP List is up and running. This is a welcome development that should increase the public's confidence in the protection of IP rights in Hong Kong. The changes are seen as a positive step in the context of IP enforcement in Hong Kong, but the city still has some catching up to do, as many of the city's neighbours in the Asia Pacific region have specialist IP courts served by a number of IP judges.



Safe As Houses – The PRC Issues Revised Draft of the Personal Information Security Specification

By Gabriela Kennedy, Partner
Mayer Brown, Hong Kong

Karen H. F. Lee, Counsel
Mayer Brown, Hong Kong

On 2 January 2018, the Standardization Administration of China ("**SAC**") released the final draft of "Information Technology – Personal Information Security Specification" (National Standard GB/T 35273-2017) (GB/T 35273-2017 信息安全技术个人信息安全规范) ("**Specification**"). The Specification came into effect on 1 May 2018. The Specification sets out the recommended practices on personal information protection. Although the Specification is not legally binding, compliance is expected by the PRC authorities and may be taken into account when assessing a company's compliance with related laws (e.g. China's Cybersecurity Law).

On 1 February 2019, China's National Information Security Standardization Technical Committee ("**NISSTC**") issued a revised draft of the Specification ("**Revised Draft**") for public consultation. The consultation period ended on 3 March 2019.

What is the effect of the Revised Draft? The Revised Draft imposes more stringent requirements on data controllers,

particularly with regard to obtaining consent. It shows a clear intent of the PRC government to give control back to individuals on how their personal information is used, and to curb the excessive collection of data and the manner in which data can be shared by companies. A summary of the key changes proposed by the Revised Draft are set out below.

Collection and Consent

Under Article 5.3 of the existing Specification (moved to Article 5.4 in the Revised Draft), where the personal information is being directly collected from a data subject, the data controller must obtain the informed consent of the data subject in relation to the collection and use of their personal information (e.g. type of personal information being collected, purpose of use, etc.). For indirect collection of personal information, the existing Article 5.5 of the Specification requires the data controller to ask the third party supplier of the personal information to verify and confirm the legitimacy of the source of the personal information, and to confirm the scope of consent obtained by the supplier from the data subject.

The Revised Draft introduces a new requirement that prohibits data controllers from coercing data subjects to agree to services or functions and associated data collection. In particular:

a. data controllers must not obtain a one-off consent from the data subject to the collection of different types of personal information in relation to the provision of a bundle of services or functions;
b. data controllers should only activate a service or function and start to collect related personal information when the data subject actively opts-in;
c. data controllers shall provide opt-out mechanisms that are as easily accessible and user-friendly as the opt-in mechanisms; and
d. if a data subject terminates, opts out or refuses to opt-in for certain functions or services, then the data controller shall not: (i) frequently ask the data subject for consent; or (ii) suspend or downgrade the functions or services that the data subject has opted-in to receive/use.

Annex C of the Revised Draft further requires the data controller to categorise their functions into "basic functions" and "extended functions". For basic functions, data controllers can obtain a single consolidated informed consent from the data subject for all basic functions. Such consent must be obtained through a positive action (e.g. submitting a form, ticking a box to indicate consent, etc.). Any amendments to a data controller's basic functions in light of any changes to their products or services, will require fresh consent to be obtained from the data subjects.

With regard to any extended functions, data controllers must obtain a separate informed consent from the data subject for *each* such extended function. Unless the data subject takes the initiative to activate the extended function, the data controller can only request consent from a data subject once in every 24 hours. Failure of a data subject to provide their consent to any extended function cannot result in the data controller downgrading or terminating the provision of any basic function.

A basic function is defined as a function that falls within the core expectations or key requirements of the data subject when they opt in to receive the relevant service or function from the data controller. The Revised Draft specifically states that functions relating to the enhancement of customer experience or research and development of new products cannot amount to a basic function.

For example, if a data subject downloads a restaurant review app provided by a data controller, then the basic function may be to enable the data subject to upload their own restaurant reviews and to access reviews and comments posted by other users on a restaurant. Other functions, e.g. to use data to create a personalised experience and to recommend restaurants, or to carry out analytics, etc., will be considered as extended functions.

Exceptions to Consent Requirement

The existing Specification provides certain exceptions to the consent requirement. For example, a data controller can collect and use personal information directly related to national security, public interest and judicial procedures, without prior consent. The Revised Draft moves Article 5.4 to Article 5.7 and further adds an exception that allows data controllers to collect and use personal information without consent, if it is required in order for the data controller to comply with their legal and regulatory requirements. However, a significant change is the deletion of the existing exception that allows the data controller to use personal information without consent, in order to execute and perform a contract with a data subject. Therefore, data controllers can no longer rely on contracts with data subjects as a ground for its data collection – the data controller would need to obtain the data subject's express consent.

Privacy Policy

The existing Article 5.6 requires a data controller to include certain information in its privacy policy, such as contact details of the data controller, the purposes of collection and use, and the purpose of any transfer. The new Article 5.6 of the Revised Draft now requires data controllers to also distinguish between the different types of personal information that will be collected for each different basic function and extended function. Any sensitive personal information that will be collected must also be highlighted.

The privacy policy should also set out the data protection policies and measures that have been implemented by the data controller in order to safeguard the personal information in its possession, and must remind data subjects of the potential risks relating to the provision of their personal information to the data controller and the consequences of failing to provide it. If any personal information will be transferred outside of China, then the privacy policy must include information regarding such cross-border transfers.

Data controllers must bring their privacy policy to the attention of the data subjects via a pop-up window whenever a data subject uses the functions or services of the data controller for the first time or registers for such function or service.

Personalisation and Targeted Advertising

The new Article 7.4 proposed in the Revised Draft regulates how data controllers provide personalised recommendations to data subjects based on their interests, transaction records, and browsing history, etc.:

a. if a data controller provides personalised news or information services (e.g. search engines, news sites, etc.), it should clearly identify the personalised results by labelling the relevant news or information with words such as "personalised display" or "targeted push", and provide the data subject with a user-friendly mechanism to opt-out of the personalised function;
b. e-commerce operators or merchants that provide personalised search results or recommendations must simultaneously also provide non-personalised recommendations and results to that consumer;
c. data controllers must provide a mechanism for data subjects to manage their preferences in relation to receiving targeted advertisements and personalised displays; and
d. when a data subject opts-out of personalised displays or targeted marketing, the data controller should provide the data subject with the option to delete or anonymize the personal information used for such purpose.

Consolidating Personal Data

When a data controller consolidates personal information of a data subject that has been collected from different sources, different purposes of use may apply. Article 7.5 of the Revised Draft requires the data controller to ensure that it still only uses each type of consolidated personal information for the relevant purpose notified and consented to by the data subject. In addition, the data controller should carry out a personal information security impact assessment and take appropriate measures to safeguard the personal information in light of the consolidation.

Third Party Access

The existing Article 8 includes provisions regarding the use of data processors, and the sharing, transfer and public disclosure of personal information. The Revised Draft adds a new Article 8.7, which imposes additional requirements when a data controller allows a third party to collect personal information through that data controller's products or services (e.g. through Application Programming

Interfaces (APIs), etc.), and such personal information will be used by the third party for its own purposes (and not as a data processor or joint controller). These requirements include the following:

a. establish restrictions, conditions and a mechanism to manage the third party's access, e.g. a security assessment;
b. specify through contractual or other means the security responsibilities of both parties and the personal data security measures to be implemented by the third party;
c. clearly notifying the data subjects of the services or products that will be provided by the third party;
d. retain relevant contracts and management records relating to the third party's access;
e. require the third party to obtain consent from the data subjects for the collection of their personal information in accordance with the Revised Draft, and verify that the third party has complied with this requirement;
f. require the third party to establish a mechanism to handle a data subject's complaints and requests;
g. monitor the third party's data security management practices, require the third party to rectify any issues and terminate the third party's access in the event of any issues; and
h. for automatic tools embedded by the third party in the data controller's products or services (such as coding, scripts, interfaces, etc.), the data controller must ensure that the data collection activity of such tools are in compliance with the agreed requirements, monitor the data collection of such tools and terminate access if its activity exceeds what was agreed.

Data Breach Notification

The existing Article 9.1 requires data controllers to formulate an emergency response plan to handle security data breaches. When an incident occurs, data controllers must keep a record of the incident, assess the possible impact, adopt necessary measures to handle, rectify and mitigate the situation, and report the incident in a timely manner in accordance with the National Cybersecurity Incident Emergency Response Plan.

In addition, the current Specification requires data controllers to notify affected data subjects of any security incident in a timely manner (no matter how small). If it is difficult to notify each affected data subject individually, then a public notice may be provided. The Revised Draft proposes to introduce a threshold, which will only require notification to be made to affected data subjects if the incident would adversely affect the data subject's rights and interests, for example if the breach involved sensitive personal information.

The Revised Draft further requires data controllers to report an incident to the Cyberspace Administration of China if it involved the personal information of more than one million individuals or it concerned sensitive personal information relevant to national security or public interest (such as genetic information, information related to biological characteristics, health records or other personal sensitive data).

Internal Management

The Revised Draft amends Article 10.1 and imposes an obligation on those responsible for the protection of personal information within the data controller, to (amongst other things) conduct personal information security assessments, provide recommendations on data protection, disclose information such as complaint and reporting mechanisms, and handle any reported incidents in a timely manner.

In addition, the Revised Draft introduces a new Article 10.2, which requires data controllers to keep a data processing record of its collection and use of personal information. The record shall include:

a. the types, quantity and sources (whether collected directly or indirectly from the data subjects) of the collected personal information;
b. the purpose of collection and use of the personal information;
c. whether data processors are involved, and whether any personal information is shared, transferred, publicly disclosed or transferred overseas; and
d. the system, organisation, and personnel involved in each step of the data processing.

Takeaway

The Revised Draft is keeping in line with the recent proactive enforcement steps being taken by the PRC Authorities to protect personal information. For example, in January 2019, the Cyberspace Administration Authority, the Ministry of Industry and Information Technology, the Ministry of Public Security and the State Administration for Market Regulation issued a joint notice on illegal data collection by mobile apps, which stated, amongst other things, that mobile app operators must not collect personal information unrelated to their services, must obtain users' consent, and must protect their data in compliance with the Cybersecurity Law. On 18 March 2019, the Jiangsu province police also stated that they have been focusing on regulating the online environment, including protecting personal information, clamping down on illicit online activities and urging network operators to comply with their cybersecurity obligations.

The Revised Draft acts as a precursor to what we can expect from the PRC's new overarching personal information protection law that is in the process of being formulated.

Data Hoarders Beware!

By Gabriela Kennedy, Partner
Mayer Brown, Hong Kong

Karen H. F. Lee, Counsel
Mayer Brown, Hong Kong

On 21 February 2019, the Hong Kong Privacy Commissioner for Personal Data ("**PCPD**") published an investigation report into a data breach which occurred in April 2018 involving a database of Hong Kong Broadband Network Limited ("**HKBN**"). The incident highlights the need for organisations to have robust data retention policies in place and regularly purge their databases and keep a clear record of how and where their data is stored.

Background

In 2012, HKBN conducted a system migration, but one of its databases was not migrated ("**Inactive Database**"). The Inactive Database contained personal information of about 380,000 customers and service applicants collected up until 2012, including names, contact details, HKID numbers and credit card information. After the system migration, the Inactive Database was taken out of use, but due to human error it was not erased and remained connected to HKBN's internal network. Unsurprisingly, no-one at HKBN remembered the existence of the Inactive Database and as a result its security or safeguarding measures were never upgraded.

In mid-April 2018, HKBN became aware that a hacker had accessed the Inactive Database. It immediately took measures to stop the breach and to notify the PCPD as well as the affected data subjects.

Data Retention

Under Section 26 of the Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**"), when personal data is no longer required for the purpose for which it was collected (or a directly related purpose), then the data user must take all practicable steps to erase the data (unless the erasure is prohibited by law or against public interest). Data Protection Principle 2 ("**DPP 2**") of the PDPO also stipulates that the data user must take all practicable steps to ensure that data is not kept for longer than necessary in order to fulfil its original purpose of collection, or a directly related purpose. Unlike the provisions of the European Union General Data Protection Regulation ("**GDPR**"), the PDPO does not provide data subjects with an express right to request the erasure of their personal data by data users.

HKBN admitted that following the system migration in 2012, it no longer needed the Inactive Database. Unfortunately, due to human oversight, HKBN took no steps to erase the Inactive Database. It also had no internal guidelines governing the system migration or any concrete policy on retention of its data. In practice, HKBN retained the personal data of former customers for 3 years following the closure and clearance of their account (after the incident this period was reduced to 6 months). Unfortunately, the Inactive Database contained personal data of some former customers that went back over 15 years.

By failing to erase the Inactive Database and retaining unnecessary personal data for an excessive amount of time, the PCPD determined that HKBN contravened DPP 2 and Section 26 of the PDPO.

Security and Safeguarding Measures

Under Data Protection Principle 4 ("**DPP 4**") of the PDPO, data users are obliged to take all practicable steps to protect personal data from any unauthorised access, use, processing or erasure, taking into consideration:

- the type of data involved and the consequences of any breach or erasure;
- where the data is physically located;
- security measures built into the hardware where the data is stored;
- the integrity, prudence, and competence of personnel with access to the data; and
- the secure transmission of the data.

While HKBN had an Information Technology Policy ("**ITP**") with requirements concerning encryption and security patches for its databases, the Inactive Database was neither encrypted nor updated with the latest security patches after it fell off HKBN's radar in 2012. The hacker used a compromised username and password of a HKBN information technology employee to gain access to the Inactive Database. This also brought into the spotlight HKBN's rather inadequate password policy. While HKBN's ITP stipulated that passwords must be changed every three months, it neither had an enforcement mechanism for the rule nor did it adopt a two-factor authentication mechanism to protect passwords that are compromised.

The PCPD found that HKBN was in breach of DPP 4.

Enforcement Notice

As a result of HKBN's breach of the PDPO, the PCPD issued an enforcement notice against HKBN requiring it to take remedial steps and to prevent a reoccurrence. In particular, HKBN was required to:

- establish clear procedures regarding the steps, time limits and monitoring measures for the erasure of personal data from inactive database after a system migration;
- establish a clear data retention policy setting out the specific retention periods of personal data of customers and service applicants, which must be no longer than is necessary for the fulfilment of the purpose of use;
- establish a clear data security policy for the regular review of user access rights and security controls for remote access;
- implement effective measures to ensure that staff are informed of and comply with the above policies and procedures; and
- delete all personal data of customers and service applicants that have been retained for longer than the retention periods specified in the newly established data retention policy.

Takeaways

In the age of "big data", companies have a tendency to collect and retain an excessive amount of data in the hope that the data may be monetised at a future date. This hoarding tendency can result in companies losing track of the data they hold. Whilst the PDPO does not currently have strong enforcement provisions in the event of a breach of the data retention or security requirements, many companies are subject to the laws of multiple jurisdictions, and could face hefty fines under other laws (e.g. under the GDPR).

Companies need to take a close look at their data collection and retention practices to minimise the amount of data being collected to what is necessary for the relevant purpose of use. Clear policies also need to be implemented setting out specific retention periods so that employees know when personal data must be deleted, with comprehensive records being maintained to ensure that no subsets of data get overlooked and lost in the sea of information that most companies now possess.

Dash Cams : A New Panopticon?

By Gabriela Kennedy, Partner
Mayer Brown, Hong Kong
Karen H. F. Lee, Counsel
Mayer Brown, Hong Kong
Eunice Wong, Associate
Mayer Brown, Hong Kong

Car cameras, also known as dash cams, have come under close scrutiny after a recent scandal involving two well-known Hong Kong celebrities caught kissing on camera, in the back of a taxi (the "**Taxi Incident**"). Whilst the sensational details of the Taxi Incident have caused a local media frenzy, questions have been raised about the legality of car cameras and the disclosure of the video to the press.

The Issues

The Taxi Incident raises a number of questions such as: (i) is the installation of car cameras by taxi and hired vehicle drivers justified?; (ii) do the images caught on car cameras amount to personal data under the Personal Data (Privacy) Ordinance (Cap. 486) (the "**Hong Kong data privacy law**")?; (iii) if the images amount to personal data, is their collection justified?; and (iv) did the driver in the Taxi Incident breach the Hong Kong data privacy law by releasing the video footage to the media?

IS THE INSTALLATION OF CAR CAMERAS JUSTIFIED?

Under the Hong Kong data privacy law, personal data can be collected only where it is necessary for a lawful purpose directly related to the function or activity of the data user, and the excessive collection of data is prohibited. Whether the installation and use of car cameras can be justified and deemed to be necessary for taxi and hired vehicle drivers to carry out their work depends on

the purpose for which they are installed (i.e. to preserve evidence in the event of a traffic accident or other incident inside the car that puts the safety of the passenger or the driver at risk) and whether there are any less privacy intrusive alternatives to achieve the same purpose.

Although the reason why car cameras are installed is for safety and security, an increasing number of taxi companies have also installed car cameras in order to deter bad customer service by taxi drivers (e.g. overcharging, taking long routes or cherry-picking customers). According to recent statistics, around 8,000 taxis (out of 18,163 taxis in Hong Kong[1]) have car cameras installed. Apart from taxis and hired vehicles, the MTR and franchised bus operators have also installed CCTV systems with recording functions in their vehicles for the purposes of crime prevention and providing timely assistance to passengers in the event of emergencies.

It is arguable therefore that the installation of the car cameras in such vehicles is necessary and justified. However, even if this is justified, the data protection principles articulated in the Hong Kong data privacy law have to be kept in mind when collecting video or audio recordings of passengers via car cameras, in particular:

- ensuring that the recordings are made in a lawful and fair manner[2] (e.g. the cameras should be overt not covert);
- deleting the recordings as soon as practicable once the purpose of collection has been fulfilled [3](e.g. if no incident or dispute has occurred, then immediately or within 24 hours);
- only using the recordings for the original purpose for which they were collected or a directly related purpose[4] (i.e. to preserve and use evidence of traffic incidents or other safety related incidents within the vehicle); and
- minimising what is recorded to solely what is necessary (e.g. consider whether video recording is sufficient and audio recording is unnecessary, or whether cameras should be placed facing forward rather than towards the passenger, etc.).

Although there is no specific guidance from the Privacy Commissioner for Personal Data (the "**Privacy Commissioner**") on the use of car cameras, the guidance note on the use of CCTV surveillance and drones ("**Guidance Note**"), issued in 2010 and revised in 2017, can equally apply to car cameras. In particular, the Guidance Note emphasises the need for explicit notification to be given to individuals that they are subject to CCTV surveillance. In the case of car cameras, a clearly visible notice affixed to either the exterior of the vehicle or in a conspicuous manner inside the vehicle (most likely behind the driver's seat) would fulfil that requirement. The notice must clearly inform the passenger that they are being filmed and the purpose of the video. The camera should not be installed in a discreet or covert location, so that the passenger is not aware at all times of when he or she is being filmed.

DO THE VIDEOS COLLECTED BY CAR CAMERAS AMOUNT TO A COLLECTION OF PERSONAL DATA AND, IF SO, IS IT JUSTIFIED?

In the landmark case of *Eastweek Publisher Ltd and Another v Privacy Commissioner for Personal Data* [2000] 2 HKLRD 83 ("**Eastweek Case**") , the Court of Appeal ruled that the photograph of a woman published in a magazine together with unflattering comments on her fashion sense did not amount to a collection of personal data under the Hong Kong data privacy law, as the journalist did not seek to identify the woman in question when the photo was taken. The Eastweek Case held that the Hong Kong data privacy law is not intended to provide a general right to privacy against all possible forms of intrusion into an individual's private sphere, but only protects the privacy of individuals in relation to personal data – a key distinction which limits the recourse of affected individuals in *Eastweek*-type situations, who seek to rely on data privacy legislation.

Post the Eastweek Case in a few decisions involving the publication of photographs taken of celebrities in their private residences, the Privacy Commissioner took the view that the Hong Kong data privacy law did engage as such photographs were taken specifically due to the identity of the well-known celebrities for their newsworthy value (i.e. the identity of the celebrities was a key part of the purpose of collection). The test of whether photographs and video footage collected from a car camera amount to personal data depends on the extent to which the purpose of collection was to identify the individual. In 2016, footage of a woman passenger breastfeeding in the back of a taxi went viral after it was uploaded onto social media by the taxi driver. It caused public outrage and raised concerns regarding the intrusion of privacy. In response to the incident, the Privacy Commissioner considered whether the taxi driver sought to collect identifiable information via his car camera. He concluded that as the identity of the passenger could not be ascertained, the case did not involve the collection of personal data and was not caught under the Hong Kong data privacy law. In the Taxi Incident, arguably the original purpose of collection was to collect footage and evidence for safety and security reasons, and the identity of the passengers was irrelevant as no steps were taken to identify them at the time of collection.

The Taxi Incident raises new issues totally different from those raised by both the Eastweek Case and the previous 'celebrity cases'. Whilst arguably the footage did not seek to identify the passengers initially, once the driver recognised them and the cloak of anonymity was pierced, did such footage not amount to the collection of personal data? In analogous cases elsewhere, a simple digital crumb that can signal a personal identifier has been held sufficient to lift the cloak of anonymity from de-identified data.

HOW MUCH FOR THE DATA IN THAT TAXI?

Under the Hong Kong data privacy law, data users must not, without the prescribed consent of the data subject, use the data collected for a new purpose (i.e. a purpose not directly related to one covered by the original notification provided at the time of collection). Prescribed consent refers to consent that is expressly and voluntarily given by the data subject.

The Taxi Incident is clearly a case of data being used for a different purpose to that for which it was collected. Had the passengers in the car not been the celebrities they are, we would not be debating now whether a passenger should have an expectation of privacy while travelling in a taxi. Is such a vehicle a private or a public space? The Privacy Commissioner has commented on the case and described taxis as semi-public places. What does this mean for the collection of personal data by car cameras? Is there an editorial obligation on the part of the taxi driver to delete content that is outside the known or expected purpose of collection/use of the data? The focus of the debate so far has centred on the clearly different purpose to which the video was put by the driver that saw a lucrative opportunity before him and seized the day (and the cash). A further interesting question in the case relates to who is the data user? The majority of taxi drivers in Hong Kong lease their vehicles from a few taxi licence holders and if the car camera belongs to the owner of the taxi then there is a further possible offence of disclosure of data that belongs to another, without their authority[5].

Takeaway Points

Public perception is a powerful thing that cannot be ignored. Whether or not the collection of passenger footage in a taxi or hired vehicle amounts to the collection of personal data, a lack of transparency in respect of such collection of data and its subsequent misuse can have significant consequences in the court of public opinion.

Ironically, in a world where almost everything is captured or shared in the virtual public space that is the Internet, people are becoming more sensitive about protecting their "right to privacy" in 'real-world' public or semi-public spaces. The expectation now is not only that companies strive to comply with well-known data privacy precepts, but that they are also sensitive to public perceptions of privacy, which more often than not go beyond what is articulated in the statute book.

1 According to the Transport Department as of May 2019.
2 DPP1(2), Personal Data (Privacy) Ordinance.
3 DPP2(2), Personal Data (Privacy) Ordinance.
4 DPP3, Personal Data (Privacy) Ordinance.
5 Section 64, Personal Data (Privacy) Ordinance.

Contact

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

Gary Hnath
Partner
+1 202 263 3040
ghnath@mayerbrown.com

Lisa Ferri
Partner
+1 212 506 2340
LFerri@mayerbrown.com

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

Karen H. F. Lee
Counsel
+852 2843 4452
karen.hf.lee@mayerbrown.com

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

Elliot Choi
Associate
+1 212 506 2235
echoi@mayerbrown.com

Scott McMurry
Associate
+1 212 506 2216
smcmurry@mayerbrown.com

Jing Zhang
Associate
+1 212 263 3385
jzhang@mayerbrown.com

Eunice Y.T. Wong
Associate
+852 2843 4286
eunice.wong@mayerbrown.com