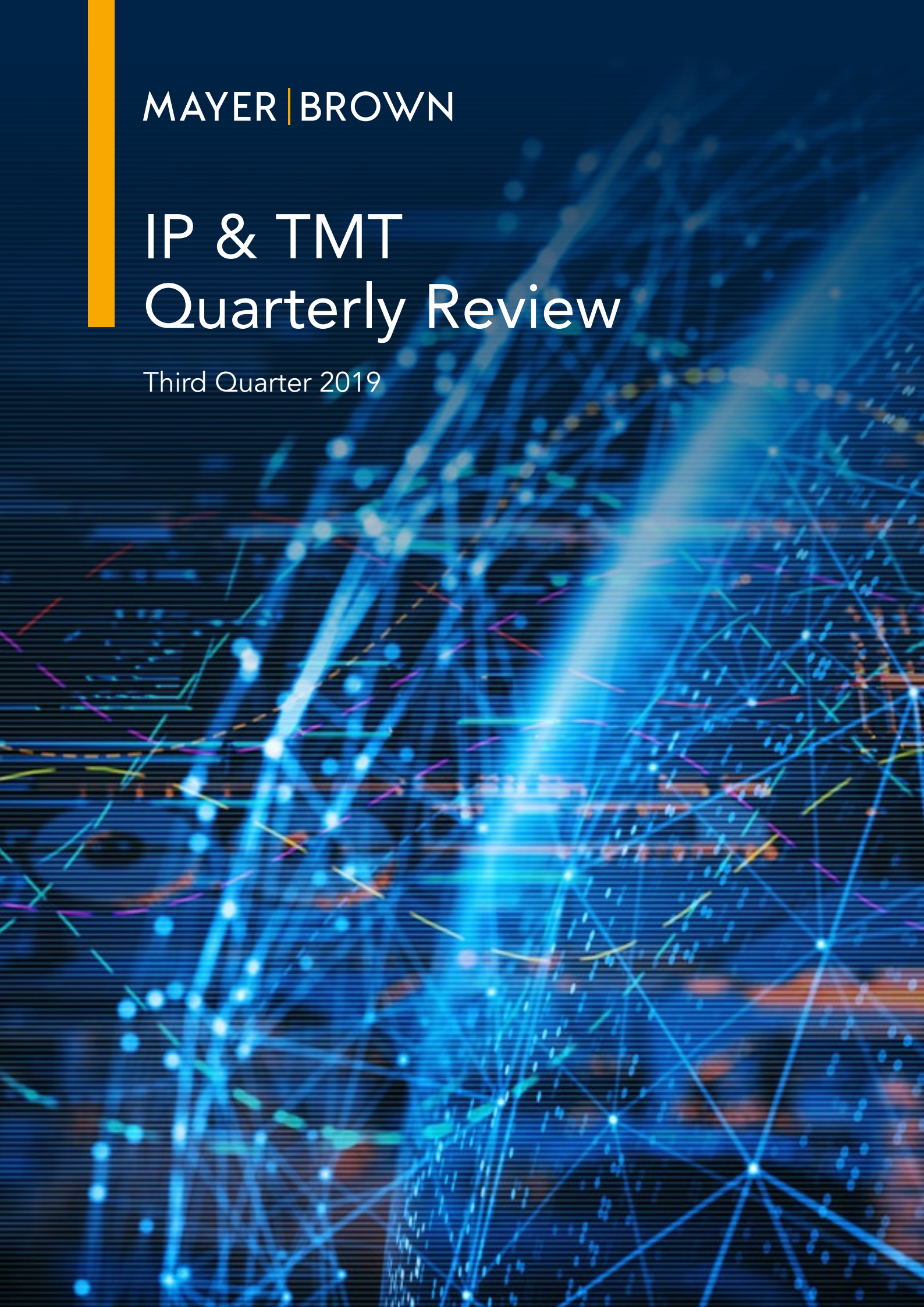
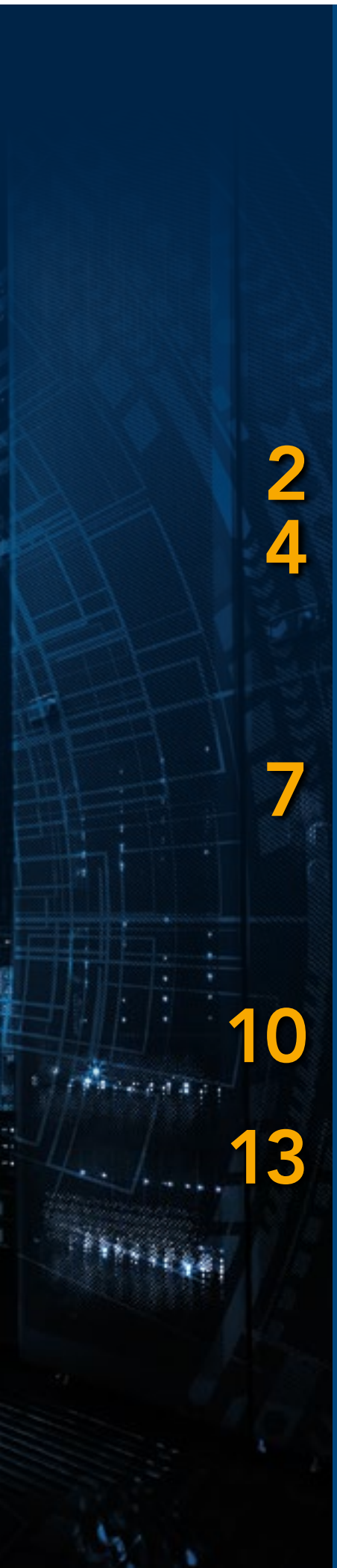
MAYER | BROWN

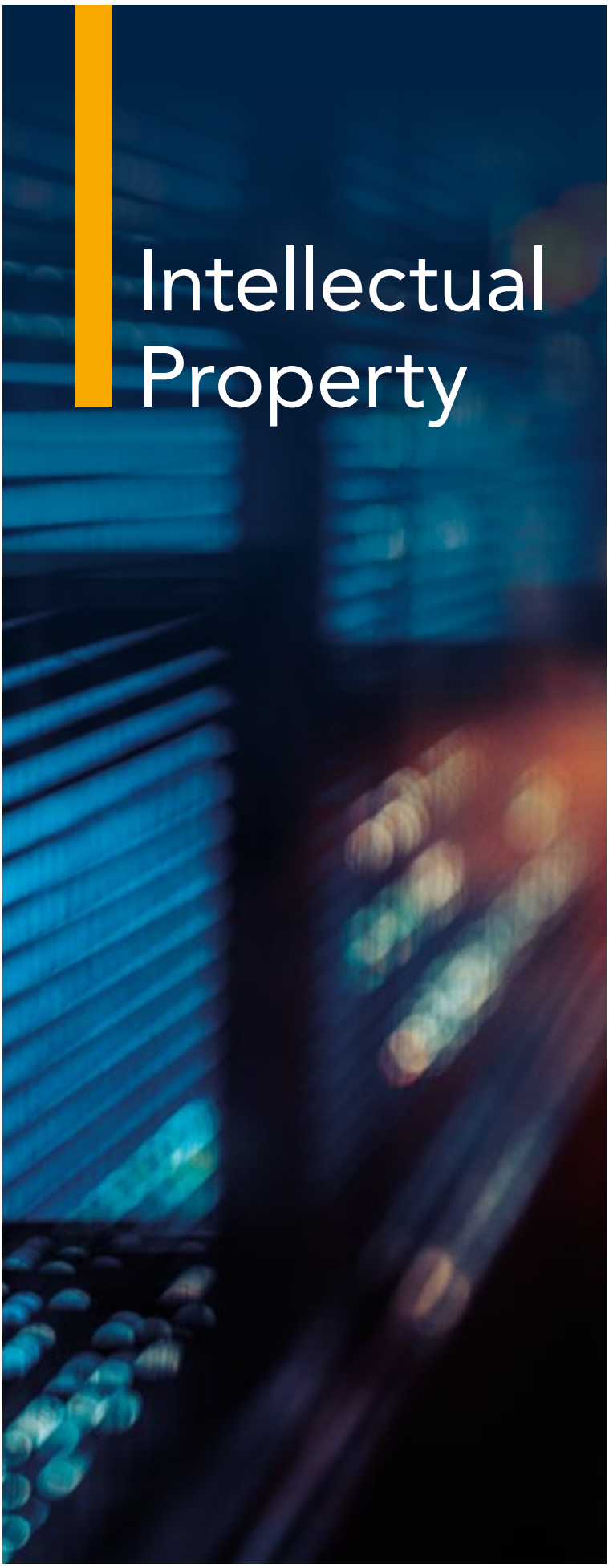
IP & TMT Quarterly Review

Third Quarter 2019



Contents





The Gift of Time: New Limitation Period for Filing a CNDRP Complaint

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

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

On 18 June 2019, the CNNIC ccTLD Dispute Resolution Policy ("**CNDRP**") was amended and the limitation period for filing a CNDRP complaint was extended from two years to three years from the date of registration of a <.cn> and <.中国> ("**cnTLDs**") domain name.

Overview of the CNDRP

The CNDRP is an alternative dispute resolution system that enables brand owners to recover cnTLD domain names registered by third parties, which incorporate the brand owner's trade mark. In order to obtain a favourable decision under the CNDRP system, a brand owner must satisfy the following three requirements:

i. the disputed domain name is identical with or confusingly similar to the complainant's name or mark in which the complainant has civil rights or interests;
ii. the respondent (i.e. registered holder of the domain name) has no right or legitimate interest in respect of the domain name or major part of the domain name; and
iii. the respondent has registered or has been using the domain name in bad faith.

The CNDRP is modelled on the Uniform Domain Name Resolution Policy ("**UDRP**") system, but with three key differences. The first element to be satisfied under the CNDRP refers to a name or mark in which the complainant has civil rights or interests. This is potentially broader than the UDRP requirement, which refers only to trade mark and service mark rights. In relation to the third element (i.e. bad faith), the CNDRP only requires the establishment of *either* bad faith registration or bad faith use. In contrast, the UDRP requires the complainant to prove both registration *and* use in bad faith.

Lastly, in 2006, the CNDRP was amended and introduced for the first time a time bar that prohibited the filing of complaints in respect of a cnTLD domain name that had been registered for more than two years. The latest changes introduced on 18 June 2019, now extend this period to three years. Unlike the CNDRP, no such limitation period is stipulated by the UDRP.

The CNDRP is a quicker and more cost efficient way of resolving a domain name dispute then having to go through court proceedings in China. Unlike court proceedings, the CNDRP does not involve a hearing, and all submissions and evidence are filed electronically, without any stringent requirements regarding the admissibility of evidence or any notarization obligations. A decision is rendered by an independent panel (either single member or three member panel), based on the written submissions and evidence provided. Decisions are usually rendered within a few months. However, damages cannot be awarded under the CNDRP system. The only remedies available to brand owners are the transfer of the disputed domain name to the brand owner, or the cancellation of the disputed domain name.

Why is the Extended Deadline Important?

Previously, any CNDRP proceedings had to be initiated within two years of the relevant cnTLD domain name being registered, otherwise the brand owner was time barred from relying on the CNDRP system. If the two year limitation period had expired, a brand owner's only chance of recovering the domain name would be through lengthy and costly court proceedings. The extension of the limitation period to three years, gives brand owners some extra time to tackle cyber squatters, but the fact remains that monitoring of domain names and sites is essential to prevent a situation where a brand owner may be time barred from seeking to recover a cnTLD domain name through cheaper and faster alternative dispute resolution mechanisms.

Does the transfer of a cnDRP domain name to a new owner reset the time limit? In Leister Brands AV v. Chen Qiuheng (HKIAC DCN-1500641), the panel held that the transfer of a domain name amounted to a new registration, which effectively restarted the limitation period for filing a complaint. The panel relied on the fact that the circumstances of bad faith registration or use of a domain name under Article 9 of the CNDRP, referred to both registration and acquisition of a domain name. In addition, the panel noted that if the assignment of a domain name does not amount to a new registration under the CNDRP, then this could indirectly encourage cybersquatting. This decision is consistent with the generally accepted position under the UDRP (i.e. a transfer constitutes a new registration). However, whilst previous decisions may have a persuasive effect, it is important to note that panels are not bound by them.

The limitation period leaves the CNDRP out of synch with other corresponding alternative dispute resolution systems.

What Should You Do?

Similar to trade mark squatting, cybersquatting in China is common place. In order to avoid missing the three year deadline, domain name watch services are essential. As the cost of registering a cnTLD domain name is relatively low, securing as many cnTLD domain names sooner rather than later might be the right strategy for any company that has business interests in China. Proactive rather than reactive steps are usually more cost effective in the long run.

The On-Sale Blues: U.S. Supreme Court Finds Patent Invalid for Prior Sale Under Confidential Terms

By **Gary Hnath, Partner**
Mayer Brown, Washington DC

Bryan Nese, Senior Associate
Mayer Brown, Washington DC

Earlier this year, the United States Supreme Court held that the commercial sale of a product subject to a confidentiality agreement can constitute an "on sale" bar under post-AIA[1] 35 U.S.C. § 102(a) which may invalidate a company's patent. *Helsinn Healthcare S.A. v. Teva Pharms. USA, Inc.*, 139 S. Ct. 628, 630 (2019). The *Helsinn* case underscores the need to decide whether to file for patent protection on a particular product before bringing it to market. The key to this strategy is working with experienced US patent counsel to evaluate potential patentable subject matter and to ensure that applications for patent protection are filed early.

A brief review of the *Helsinn* decision, and its implication for companies doing business in the United States, follows.

1 Certain provisions of the 2011 America Invents Act ("AIA"), including § 102, apply only to patent applications with an earliest effective U.S. filing date on or after March 16, 2013. For other applications, the pre-AIA provisions apply.

The Background

Sometime in 2001, Petitioner/Patentee Helsinn Healthcare S.A. entered into contractual agreements with third-party MGI Pharma, Inc. for the sale of palonosetron—the active ingredient in a drug used to treat chemotherapy-induced nausea. *Helsinn*, 139 S. Ct. at 630-31. Under these agreements, MGI was allowed to market and sell 0.25 and 0.75 mg doses of palonosetron. *Id.* at 631. However, MGI was to keep confidential any proprietary information of Helsinn, including the dosage amount. *Id.*

In January 2003, Helsinn filed a provisional US patent application, which covered the 0.25 and 0.75 mg doses. *Id.* That application eventually led to the patent at issue in this appeal: U.S. Patent No. 8,598,219 (the "'219 patent"). *Id.*

When Helsinn discovered that Teva Pharmaceuticals planned to sell 0.25 mg doses of palonsetron in 2011, it sued Teva for infringement of the '219 patent. *Id.* As part of its defense to those infringement allegations, Teva argued that Helsinn's 2001 sales of 0.25 mg doses of palonsetron to MGI served as an on-sale bar that rendered the '219 patent's claims invalid. *Id.*

Prior Precedent

Under both the AIA and the prior versions of 35 U.S.C. § 102, a patentee cannot obtain a patent when a product embodying that patent was sold more than a year before the patent's earliest effective filing date. For example, if a company began selling the product in 2000 but did not file for a patent on the product until 2003, that company's sales could be used to invalidate its own patent. For decades, U.S. patent practitioners have referred to this as the "on-sale" bar.

Following the enactment of the AIA, the on-sale bar provision appears in § 102(a)(1): "A person shall be entitled to a patent unless … the claimed invention was … in public use, on sale, or otherwise available to the public before the effective filing date of the claimed invention." post-AIA 35 U.S.C. § 102(a)(1). The pre-AIA version of § 102 omitted the phrase "or otherwise available to the public," but included the same "on sale" language as in the post-AIA § 102. *See* re-AIA 35 U.S.C. § 102 ("A person shall be entitled to a patent unless— (a) the invention was known or used by others in this country… or (b) the invention was … in public use or on sale in this country….").

In the context of the pre-AIA on-sale bar provision, the Federal Circuit repeatedly held that "secret sales" could be found to trigger an on-sale bar. *See, e.g., Special Devices, Inc. v. OEA, Inc.*, 270 F.3d 1353, 1357 (Fed. Cir. 2001); *Woodland Trust v. Flowertree Nursery, Inc.*, 148 F.3d 1368, 1370 (Fed. Cir. 1998).

The Court's Decision

In *Helsinn*, the Supreme Court took up the following questions: Does a sale under confidential terms constitute an on-sale bar under the post-AIA version of § 102(a)? Or did the AIA change the law so that only public sales would now constitute an on-sale bar?

In addressing these questions, the Supreme Court in *Helsinn* affirmed its earlier decision in *Pfaff v. Wells Electronics, Inc.*, 525 U.S. 55 (1998). *Pfaff* set forth the standard for determining whether something was "on sale" under the pre-AIA § 102(a), holding that an invention was "on sale" for this purpose when it was "the subject of a commercial offer for sale" and "ready for patenting." 525 U.S. at 67. The Supreme Court's ruling in *Helsinn* did not disturb that standard.

The *Helsinn* Court then ruled that the same pre-AIA precedent applied to the AIA version of § 102(a) because both provisions use the same "on sale" language: "we presume that when Congress reenacted the same language in the AIA, it adopted the earlier judicial construction of that phrase." 139 S. Ct. at 633-34 (citations omitted). The Court rejected Helsinn's argument that the AIA's addition of "or otherwise available to the public" somehow changed the meaning of "on sale." *Id.* at 634 ("Given that the phrase 'on sale' had acquired a well-settled meaning when the AIA was enacted, we decline to read the addition of a broad catchall phrase to upset that body of precedent.").

Because *Pfaff* "did not further require that the sale make the details of the invention available to the public," and because the Court found no reason to depart from the pre-AIA interpretation of "on sale," it concluded that "a commercial sale to a third party who is required to keep the invention confidential may place the invention 'on sale' under the AIA." *Id.* at 630.

It's important to understand what *Helsinn* didn't decide. *Helsinn* didn't consider a situation where the sale itself was kept confidential. In fact, the patentee (Helsinn) and third-party purchaser (MGI) issued press releases about their agreements. *Id.* at 631. MGI even provided redacted copies of the parties' licensing and purchase agreements in its filings with the U.S. Securities and Exchange Commission. *Id.*

Takeaways

Helsinn reaffirms the importance of carefully evaluating your company's intellectual property strategy regularly and limiting disclosures that could possibly create an invalidating on-sale bar. Specifically, to minimize the risk of losing patent rights due to an on-sale bar, companies should work with experienced U.S. counsel to, for example:

i. evaluate the potential patentability of new products before offering those products for sale;
ii. put into place internal procedures for the disclosure and evaluation of potential patentable inventions; and
iii. prepare and file timely provisional patent applications with the U.S. Patent and Trademark Office for any new innovations.

While the AIA provides for a one-year "grace period" for certain types of disclosures (*see* post-AIA 35 U.S.C. § 102(b)), companies seeking the strongest protection for their patent rights should work to file a patent application before products are brought to market. Failure to do so creates a risk of jeopardizing a company's patent rights when doing business in the United States.

More Changes on the Horizon: New Cross-Border Transfer Restrictions and Personal Information Requirements in the PRC

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

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

Despite being brought into force over two years ago, uncertainty remains regarding the application of China's Cybersecurity Law ("**CSL**"). This largely stems from the fact that many of the supplemental measures and guidelines issued by the Chinese authorities still remain in draft format.

On 28 May 2019 and 13 June 2019, respectively, the new draft Measures for Data Security Management ("**New Draft Security Management Measures**") and the new draft Measures on Security Assessment of the Cross-Border Transfer of Personal Information ("**New Draft Cross-Border PI Measures**") were issued for public consultation. These recent drafts appear to depart significantly from the draft Security Assessment Measures for the Cross-Border Transfer of Personal Information and Important Data, which were issued in 2017. More stringent and detailed requirements now appear to be the norm, particularly regarding the cross-border transfer of personal information and important data.

Application

The CSL applies to critical information infrastructure ("**CII**") operators and network operators in China. CIIs include key sectors such as finance, transportation, utilities (e.g. energy and water), government and communications, and any other industries that the Chinese authorities identify as having the potential to cause serious damage to national security, national economy and people's livelihood and public interests in the event they suffer a security breach leading to any destruction, loss of function or data. In the past year or so, additional sectors that have been identified by the Chinese authorities as falling into the CII category, they include media, e-commerce, e-payment, search engines, emails, blogs, cloud computing, enterprise systems and big data.

As far as network operators are concerned, the definition is broad enough to essentially include any business that uses some form of IT infrastructure in China (i.e. owns or operates a computer network, server or website in China), regardless of its industry sector.

Transfers of Personal Information and Important Data

Under the New Draft Cross-Border PI Measures and the New Draft Security Management Measures, a CII operator or network operator cannot transfer or disclose personal information or important data collected or generated during their operations in China to anyone outside of China, unless:

a. they have completed an official security assessment;
b. a contract is signed with the intended recipient (which must incorporate specific provisions stipulated by the New Draft Cross-Border PI Measures); and
c. for personal information, the express and informed consent of the relevant individual is obtained.

In addition, the prior authorisation of the relevant regulatory authority is also required for the cross-border transfer, disclosure, sale or publishing of important data by CII operators or network operators. The definition of "important data" under the New Draft Security Management Measures only covers data which, if leaked, may directly affect national security, economic security, social stability, public health and security, such as non-public government information, large-scale population, genetic health, geographic and mineral resources. The definition expressly excludes any information relating to the production, operation or internal management of an entity and personal information.

The above restrictions appear to have extra-territorial effect and may apply to companies that do not have a physical presence in China, but which have operations that involve the collection of personal information of Chinese residents. In particular, the New Draft Cross-Border PI Measures provide that if the business activities of any organisation located outside China results in the collection of personal information of persons located in China, then such organisation will be subject to the New Draft Cross-Border PI Measures as a network operator.

Under the previous draft measures, CII operators and network operators were required to carry out a self-assessment for the cross border transfer of personal information, and an official security assessment by the relevant local authorities would only be necessary if certain thresholds were met or the transfer was being made by a CII operator. In contrast, the New Draft Cross-Border PI Measures now requires all cross-border transfers of personal information by either a CII operator or network operator to undergo an official security assessment by the relevant Cyberspace Administration of China ("**CAC**") branch office. There is currently no minimum threshold in relation to the application of this requirement. In addition, no express exceptions are made in relation to intra-group transfers.

The official security assessment must be conducted prior to the cross-border data transfer, and must be completed for each different recipient. However, multiple or ongoing transfers to the same recipient will not require additional assessments. The assessment must be repeated every two years or whenever there is a change in the purpose, type or retention period regarding the data.

The documents that must be submitted by the CII or network operator when applying for an official security assessment will include a detailed report on the security risks and measures related to the transfer, the agreement with the intended recipient

and a declaration form. If the results of the assessment reveal that the cross-border transfer could present a risk to national security, damage public interest or provide inadequate protection for the personal information, then the transfer will be prohibited. Whilst the CII or network operator can file an objection to the decision, there is currently no detailed appeal procedure set out in the New Draft Cross-Border PI Measures.

A record must be retained by CII operators and network operators for at least five years, which details all of their cross-border transfers of personal information. The local CAC office is obligated to carry out regular inspections of such records, and an annual report must also be submitted to the local CAC office regarding the CII or network operator's cross-border transfers and any related contract.

Lastly, prior to the sharing of personal information with a third party, under the New Draft Security Management Measures CII operators and network operators need to conduct an assessment of the potential security risks and to obtain the express consent of the data subjects. This requirement is not expressly limited to cross-border transfers and does not exclude intra-group sharing of personal information – therefore it appears that it may also apply to domestic transfers and transfers within the same group. There are certain exceptions to this requirement, including situations where the data was collected from a public source and the sharing is not in violation of the data subjects wishes, the data subject voluntarily published his personal information, it is necessary for law enforcement purposes or to protect national security, and so on.

Personal Information

Outside the context of cross-border transfers, the New Draft Security Management Measures impose further obligations on CII operators and network operators in relation to personal information. Unlike the "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) ("**PI Specification**"), and its draft amendments released on 1 February 2019[2], the New Draft Security Management Measures (once finalised and brought into operation) will be legally binding and a breach could lead to various penalties (including the shutting down of business operations). The New Draft Security Management Measures introduce requirements such as the need to obtain explicit and informed consent of the data subjects (and specifically sets out the information that needs to be provided to the data subject), an obligation not to force or mislead data subjects to provide their consent (e.g. bundled consent, default consent, etc.), not to take any discriminatory actions based on the scope of consent provided by the data subject (e.g. reduce service quality), comply with data access requests, implement data encryption and backup measures, and so on.

In addition, CII operators and network operators that collect important data or sensitive personal information for business purposes must also file with their local CAC office their rules for collection and use, and the purpose, scope volume, method, type and retention period of such data. The CII operators and network operators must also designate a person to be in charge of the data security for the important data and sensitive personal information.

Where to Now?

The draft measures are likely to be finalised by the end of 2019. For now, companies that have a link to China (e.g. business operations in China, networks in China, collecting information from Chinese residents, Chinese-hosted website, vendors in China, etc.), are advised to conduct privacy and security audits to ensure compliance with the CSL. In particular, companies should carefully scrutinise where their data is held, and engage in conversations with their supply chain.

2 See our article entitled Safe As Houses – The PRC Issues Revised Draft of the Personal Information Security Specification found here: https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2019/06/asi_ip_tmt_quarterlyreview_2019q2.pdf

Doxing: The New Frontier for Data Breaches in Hong Kong?

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

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

In recent months Hong Kong has made international headlines. Less widely circulated news is that between June and September 2019, the Hong Kong Privacy Commissioner for Personal Data ("**PCPD**") has investigated over 1,000 cases of doxing that mainly involved the personal data of police officers and their family members, in the wake of the Hong Kong protests. As of 4 September 2019, 692 cases have been referred by the PCPD to the police for investigation.

Background

Since June this year, the personal data of police officers, government officials, legislators and their respective family members ("**Individuals**") has been circulated online across various forums, social media platforms and instant messaging platforms, for the purpose of encouraging cyber bullying and harassment. The information disclosed online includes names, phone numbers, addresses, Hong Kong identity card numbers and photos (the "**Data**"). The Individuals have reported receiving nuisance calls and threats against them and their families following the release of their Data.

The PCPD has taken steps to try and take down the Data, including writing to at least 9 online platform operators asking them to remove 1,058 links. Since 4 September

2019, 45% of the links have been removed. The PCPD has issued several warnings that the persons responsible for circulating the Data online may be in breach of the Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**") and could be found guilty of an offence. So far, at least 19 people have been arrested in connection with these doxxing activities, and charged with a variety of crimes. Charges have ranged from criminal intimidation, accessing a computer with dishonest intent, and the disclosure of personal data without consent in breach of section 64 of the PDPO (discussed further below).

The Hong Kong Data Privacy Law

Freedom of speech and freedom of expression are fundamental rights under the Hong Kong Basic Law. However, a balance has to be struck between such fundamental rights and the legal restrictions relating to data privacy enshrined in laws such as the Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**"), which protects the collection, use and handling of personal data by data users in Hong Kong (i.e. the entities who control the collection, use and processing of the personal data).

The PCPD has commented that persons involved in the dissemination of the Individuals' Data (the "**Disseminators**") are likely to be in breach of the PDPO:

a. for collecting the Data in an illegal or unfair manner (breach of data protection principle ("**DPP**") 1);
b. for using the Data (including Data collected in the public domain) for a new purpose not directly related to the original purpose of collection, without the explicit consent of the Individuals (breach of DPP 3); and
c. for disclosing the Data collected from a data user (e.g. the source of the publicly available Data), without the consent of that data user, which causes psychological harm to the Individuals (regardless of the intent of the Disseminator) (breach of section 64 of the PDPO).

Breaches of the data protection principles under the PDPO do not amount to an offence. Instead, such breaches may trigger an enquiry from the PCPD or even a full-blown investigation, which in turn may lead to the PCPD issuing enforcement notices requiring corrective measures to be taken (e.g. the take down of the Data posted online). A failure to comply with an enforcement notice amounts to an offence which can attract a maximum fine of HK$ 50,000 and 2 years imprisonment (and a daily fine of HK$ 1,000 for a continuing offence), on first conviction. By contrast, the disclosure of the Data without the consent of the data user in breach of section 64 of the PDPO is an offence which attracts a maximum fine of HK$ 1,000,000 and 5 years imprisonment.

Breach of Data Privacy Law?

The PCPD has commented that the disclosure of the Data for the purposes of bullying, incitement and intimidation, is clearly unfair and illegal, and the consent of the Individuals had obviously not been obtained for this new collection and use of the Data in breach of DPP 1 and DPP 3 of the PDPO. Originally, most of the Data had been collected by the Disseminators from publicly available sources (e.g. the Individuals' personal social media accounts, phone directories, etc.). It is a common misconception that publicly available data can be collected and re-used for any purpose. This is simply incorrect. Any personal data that is made publicly available is usually disclosed for a specific purpose, e.g. the Individuals post photos of their family online to share with their friends. Any new use of that publicly available personal data must be sanctioned by the data subject (i.e. the individual who can be identified from the data) and possibly the original data user (i.e. the original person who made the personal data publicly available). Individuals who post their Data online (e.g. on social media accounts or forums), are both data users and data subjects. Any collection of such Data and subsequent posting online without obtaining the necessary consent, amounts to an offence under section 64 of the PDPO.

Not only may the Disseminators face enforcement action and criminal prosecution, the Individuals also have an express right under the PDPO to seek compensation from the Disseminators for any damages suffered (including "injury to feelings").

Does the fact that the websites or forums used to circulate the Data are hosted on servers located outside Hong Kong matter? Ultimately, so long as the Disseminators carried out their activities whilst

in Hong Kong, the Disseminators remain liable under the PDPO, irrespective of where the websites or forums, etc. used to circulate the Data are hosted.

Limited Powers of the PCPD

The PCPD has raised concerns regarding the limited statutory powers available to him in order to effectively deal with cases of doxing. In particular, unlike in other jurisdictions (such as the EU or Singapore), the PCPD does not have the power to impose administrative fines or penalties – he only has the power to issue enforcement notices, effectively giving people a "second chance" regardless of the seriousness of the breach. Even if an offence has been committed (e.g. breach of an enforcement notice or section 64 of the PDPO), a fine can only be imposed after criminal investigation and court prosecution. The ability of a data protection authority to issue administrative fines is often seen as an effective deterrent and enforcement tool, and a more efficient and cost-effective way of handling breaches then going through the traditional court procedure.

Whilst the PCPD has been issuing requests to online platforms to take down links to the Data being circulated for unlawful purposes, the PCPD has limited powers in the face of any non-compliance (particularly if the online platform is not based in Hong Kong). The PDPO does not have extra-territorial affect and (unlike in the EU, Singapore and Australia) does not directly impose liability on data processors (i.e. those who process personal data on behalf of another, and not for their own purposes). In most cases, the Disseminators will be seen as the data users and liable under the PDPO for the doxing activities, as they control the dissemination of the Data. In contrast, the online platforms are just data processors, as they only distribute the Data on behalf of and under the instructions of the Disseminators. As a result, if the PCPD (or Police) are unable to identify and locate the relevant Disseminators, limited assistance can be provided to Individuals regarding the taking down of their Data.

Where to Now?

Given the PCPD's vexing experience in handling these widespread doxing activities, it is likely that he will propose further amendments to the PDPO, seeking increased powers of investigation and enforcement, and a different regime for data processors more akin to that in the EU. It is essential for a data privacy regulator to keep up with the pace of legislative development elsewhere in order to ensure Hong Kong's continued competitiveness.

The take-away from this episode is that public data is not free data. Before taking any public data and re-using it, due regard must be given to the original purpose of this data being made publicly available, and the reasonable expectations of the data subjects in respect of it.

Contact Us

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

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

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

Bryan Nese
Senior Associate
+1 202 263 3266
bnese@mayerbrown.com

Mayer Brown is a distinctively global law firm, uniquely positioned to advise the world's leading companies and financial institutions on their most complex deals and disputes. With extensive reach across four continents, we are the only integrated law firm in the world with approximately 200 lawyers in each of the world's three largest financial centers—New York, London and Hong Kong—the backbone of the global economy. We have deep experience in high-stakes litigation and complex transactions across industry sectors, including our signature strength, the global financial services industry. Our diverse teams of lawyers are recognized by our clients as strategic partners with deep commercial instincts and a commitment to creatively anticipating their needs and delivering excellence in everything we do. Our "one-firm" culture—seamless and integrated across all practices and regions—ensures that our clients receive the best of our knowledge and experience.

Please visit mayerbrown.com for comprehensive contact information for all Mayer Brown offices.

This Mayer Brown publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek legal advice before taking any action with respect to the matters discussed herein.

Mayer Brown is a global services provider comprising associated legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England), Mayer Brown (a Hong Kong partnership) and Tauil & Chequer Advogados (a Brazilian law partnership) (collectively the "Mayer Brown Practices") and non-legal service providers, which provide consultancy services (the "Mayer Brown Consultancies"). The Mayer Brown Practices and Mayer Brown Consultancies are established in various jurisdictions and may be a legal person or a partnership. Details of the individual Mayer Brown Practices and Mayer Brown Consultancies can be found in the Legal Notices section of our website. "Mayer Brown" and the Mayer Brown logo are the trademarks of Mayer Brown.

© 2019 Mayer Brown. All rights reserved.

Attorney Advertising. Prior results do not guarantee a similar outcome.

Americas | Asia | Europe | Middle East

mayerbrown.com