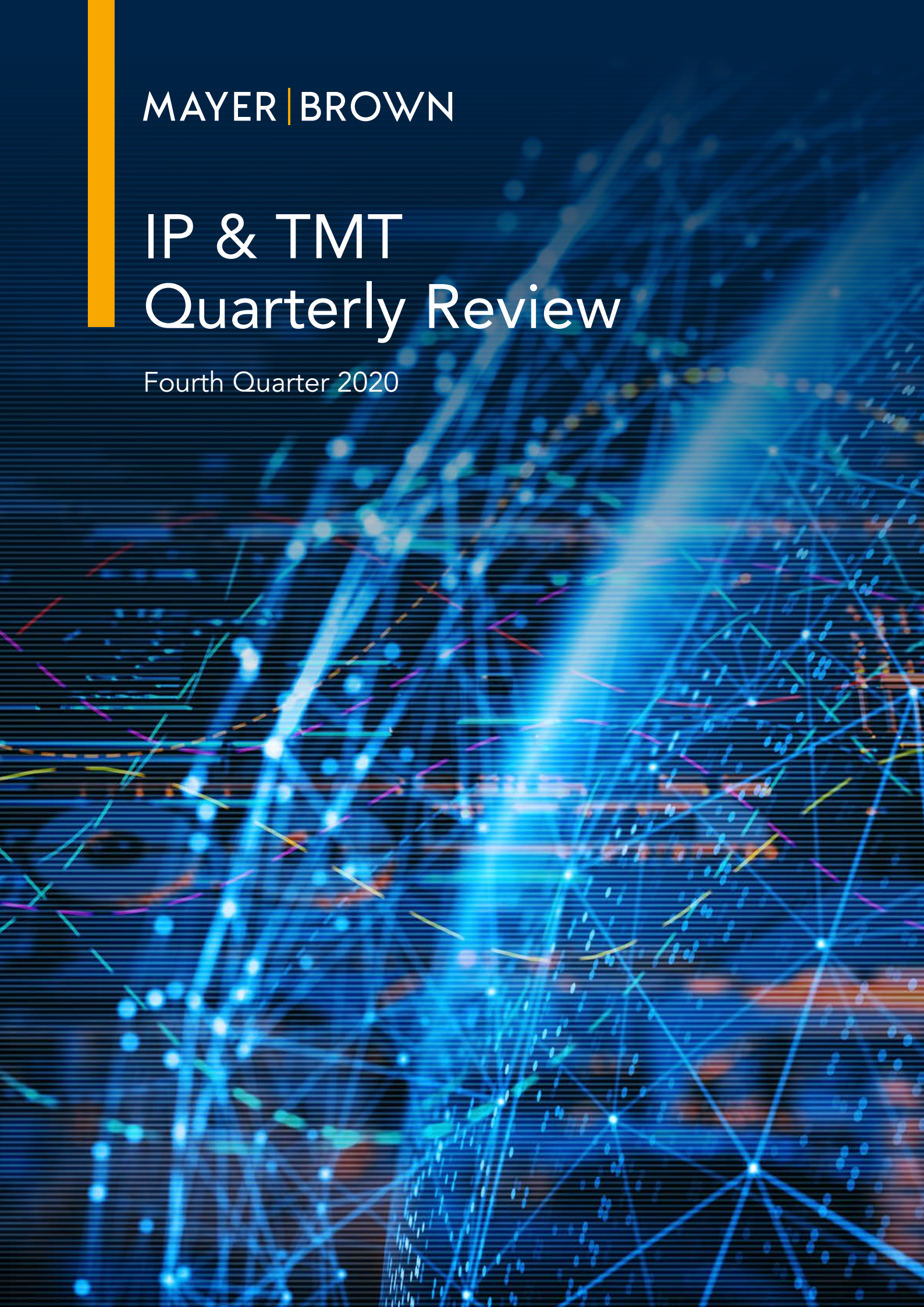
MAYER | BROWN

IP & TMT Quarterly Review

Fourth Quarter 2020



Contents

Privacy in Politics and the Politics of Privacy

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

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

Cheng Hau Yeo, Associate
Mayer Brown, Singapore

Amongst the backdrop of Hong Kong's political situation, issues concerning personal data privacy have been on the rise. In October 2020, a former technician at a telecommunications company became the first individual convicted for doxing, whilst a journalist was arrested in November for providing false statements when conducting a public search for the personal data of vehicle owners.

Doxing

The widespread occurrence of "doxing", over the last year has left local authorities struggling to find a way to reign in and deter such behaviour. Personal data of police officers, government officials, legislators and their respective family members have been circulated online in order to encourage cyber bullying and harassment. As of the end of October, the Office of the Privacy Commissioner for Personal Data ("**PCPD**") had issued over 200 requests to websites, social media platforms and online forums asking for the takedown of more than 3,500 doxing related links.

On 9 October 2020, a former technician at a telecommunications company, was found guilty of three counts of obtaining access to a computer with a view to dishonest gain for himself or another under section 161 of the Crimes Ordinance (Cap. 200) ("**CO**"), and one count of disclosing personal data obtained without consent from data users in

breach of section 64 of the Personal (Data) Privacy Ordinance (Cap. 486) ("**PDPO**"). He was the first person in the city to receive a criminal conviction for doxing. Both offences each carry a maximum sentence of five years' imprisonment.

During the trial, the District Court Judge held that the technician took advantage of his position at his former employer, by using the company's computer system to obtain the personal information of three public figures, 20 police officers and six of their family members, and to record 63 addresses without authorisation. He then went on to circulate information about a police inspector's father in an online doxing group via an instant messaging app. As a result of this incident, the District Court Judge found that the inspector's father suffered from psychological distress due to concerns over the safety of his family members and himself. The defendant was sentenced to a total of two years imprisonment, including 18 months for breach of section 64(2) of the PDPO. Separately, two individuals were sentenced this year to 28 days' imprisonment (suspended for one year) for contempt of court due to violations of doxing-related injunctions.

Whilst there is no direct offence for doxing, prosecutors can generally rely on either section 64 of the PDPO or section 161 of the CO to sanction doxing behaviour.

SECTION 64 OF PDPO

Under section 64 of the PDPO, a person commits an offence if they disclose the personal data of an individual obtained from a *data user*, without the *data user's* consent, with the intent to obtain a gain or cause a loss, or which causes psychological harm to the individual regardless of intent.

A data user is anyone who controls the collection, holding, processing or use of personal data. This could be the data subject themselves (e.g. where the individual shares their own personal data on social media), service providers of the data subject (e.g. telecommunication companies, banks, etc.) or even government authorities and regulators (e.g. marriage registry, companies registry, land registry, transport department, etc.).

In the present case, the defendant was successfully convicted as he had obtained the personal data from his employer, a telecommunications company (the data user), without its permission.

However, in less clear cut cases, the PCPD and prosecutors have found it a challenge to curb doxing activities, especially where the personal data is not obtained from the data user directly.

In contrast to Hong Kong, doxing-related provisions in other jurisdictions, such as New Zealand and Singapore, do not impose any requirements to prove that the perpetrator had unlawfully obtained the relevant personal data from a data user. Instead, the prosecutor simply has to show that the perpetrator had intended to cause harm to the victim, regardless of whether the victim's information had been obtained unlawfully.

Other than section 64 of the PDPO, individuals who disseminate personal data could be found in breach of:

a. data protection principle 1, for collecting the data in an illegal or unfair manner; or
b. data protection principle 3, for using the data (including data collected from the public domain), for a new purpose not directly related to the original purpose of collection, without the explicit consent of the individual concerned.

Unlike section 64, breaches of the data protection principles under the PDPO do not constitute an offence. Instead, they may trigger an enquiry or investigation by the PCPD, 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.

The powers granted to the PCPD to tackle doxing activities are limited. Whilst the PCPD can refer potential criminal cases to the police for investigation and prosecution, the PCPD does not have the power to issue administrative fines or penalties, and cannot order operators of websites, social media platforms or forums to takedown any content that violates the PDPO.

In January 2020, proposals were issued to amend the PDPO, including granting the PCPD the power to order online platforms to remove content, as well as the power to issue administrative fines and carry out her own criminal investigations and prosecutions. An amendment bill is expected to be issued

next year. Whilst the proposed amendments have generally been welcomed, questions have been raised as to whether such powers could be used to erode freedom of speech. A lot will turn on the wording of the bill, and the scope of the powers that will be granted to the PCPD.

SECTION 161 OF THE CO

In addition to section 64 of the PDPO, the defendant in the present case was also found guilty of obtaining access to a computer with a view to dishonest gain for another, in breach of section 161(1) of the CO. The defendant had accessed his employer's computer system, in order to obtain the personal information of police officers and public figures. However, in situations where doxers use their own computers or smartphones to engage in doxing activities (e.g. to circulate the personal information online), prosecutors will not be able to rely on section 161 of the CO. In a ruling by the Court of Final Appeal in April 2019[1], the court upheld the decision that an offence under section 161 of the CO cannot apply to a person using their own smartphone or computer to commit the alleged act, as the *actus reus* for the offence (i.e. obtaining access to a computer) would only be satisfied if it involves access to another person's computer.

Use of Publicly Available Data

Hot on the heels of the first ever conviction for doxing came the arrest of a Radio Television Hong Kong journalist in November this year. Whilst conducting research for an investigative report on what has come to be known as the "Yuen Long mob attack" which took place during the anti-government protests in July 2019, the journalist carried out searches on a public database to find out the personal details of registered owners of vehicles sighted at the incident.

The journalist has been accused of breaching section 111(3) of the Road Traffic Ordinance (Cap. 374) ("**RTO**"). Under section 111(3) of the RTO, it is an offence to knowingly make a materially false statement, when applying to obtain information from the Transport Department. When applying to obtain information from the public database, applicants must indicate the purpose of the search, which is limited to: (i) legal proceedings, (ii) the sale and purchase of vehicles, or (iii) other traffic and transport related matters. Applicants are also required to confirm that they will only use the personal data collected for activities relating to traffic and transport matters. In this case, the journalist had allegedly breached section 111(3) of the RTO as she had used the information obtained for an investigative television report, and not for the purpose indicated in her application to the Transport Department.

It is a common misconception that personal data which is publicly available can be freely used for any purpose. Under the PDPO, anyone who collects personal data from a public database and uses it for a new purpose (e.g. conducting land searches to then distribute the information for doxing purposes), may commit an offence under section 64 of the PDPO or be in breach of data protection principle 3 (i.e. using personal data for a purpose not directly related to the original purpose of collection, and without the data subject's consent). However, the PDPO provides a defence against the section 64 offence and an exemption to data protection principle 3, if the use of the personal data is for a news activity that is in the public interest. This is likely to be the reason why the journalist was not charged with a breach of the PDPO, and instead was charged with committing an offence under section 111(3) of the RTO.

Takeaways

Controversial issues relating to personal data privacy have been in the news over the last year, with a growing number of concerns relating to doxing, freedom of speech and access to data under the new National Security Law. The balance between protecting personal data versus freedom of speech and national security will be tested in the near future, with the outcome of the case against the journalist and the proposed amendments to the PDPO having major implications for data privacy in Hong Kong.

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

1 *Secretary for Justice v Cheng Ka Yee and others* [2019] HKCFA 9

Practical Lessons from the Jury Verdict in *Motorola v. Hytera*

By **Gary M. Hnath, Partner**
Mayer Brown, Washington D.C.

Jing Zhang, Partner
Mayer Brown, Washington D.C.

Earlier this year, following a trial that spanned over several months, an Illinois federal jury found Hytera liable for trade secret misappropriation and copyright infringement and awarded Motorola $345.8 million in compensatory damages and $418.8 million in punitive damages, for a total of $764.6 million. The jury deliberated for only a little more than two hours before reaching the unanimous verdict and awarded the maximum amount requested by Motorola.

Like many other high-stakes litigations involving intellectual property rights, this case has been hard fought. By the time the parties started jury selection on November 6, 2019, almost two and a half years had passed since Motorola filed its initial trade secret misappropriation claim and fifteen months had gone by since Motorola amended its complaint to also allege copyright infringement. We discuss below the global battle between these two major competitors, the facts and strategies relating to the Illinois case and trial, and some lessons to be learned for Chinese technology companies.

The Global Litigation War Between Motorola and Hytera

The Illinois verdict is the latest chapter in a global war between Motorola and Hytera spanning at least six legal proceedings in the U.S. and Europe over the last four years. This reflects a growing trend where litigation disputes between companies are often not confined to just one case, but become part of a world-wide multi-jurisdictional campaign.

Motorola filed its complaint for trade secret misappropriation against Hytera in Illinois on March 14, 2017. While that case has been pending, Motorola secured wins against Hytera in Germany in two patent infringement actions (one in Mannheim and the other in Düsseldorf) and a partial win in a Section 337 investigation at the U.S. International Trade Commission (Inv. No. 337-TA-1053), each time forcing Hytera to either disable and/or redesign certain features and functionalities in its accused products.

The legal battle between the parties is far from over. Motorola is also pursuing another patent infringement action against Hytera in the US District Court for the Northern District of Illinois (Case No. 1-17-cv-01972), which involves the same seven patents that were previously in dispute between the parties in the ITC investigation. Fact discovery closed in May this year.

In response to the series of legal actions filed by Motorola around the globe, Hytera has counterattacked. It filed its own patent infringement action against Motorola in the US District Court for the Northern District of Ohio (Case No. 1-17-cv-01794), alleging infringement of Hytera's patent covering an "Intelligent Audio" feature in certain Motorola two-way communication devices.

Additionally, Hytera filed an antitrust and unfair competition action against Motorola in the US District Court for the District of New Jersey on December 4, 2017 (Case No. 2-17-cv-12445), which has since been transferred to the Northern District of Illinois at Motorola's request (Case No. 1:19-cv-00176).

Factual Background of the Illinois Case

The most important chapter of this global battle began with Motorola's complaint in Illinois in 2017. Motorola and Hytera are competitors in the digital two-way radio market. As the parties stipulated in jury instructions filed in the case, Motorola launched its MotoTRBO professional digital radios in 2006 and first sold them in early 2007. Hytera then launched its DMR professional radios in early 2010. Dkt. 895. Motorola's complaint in that case revolved around the activities of three former Motorola employees Gee Siong Kok ("G.S. Kok"), Yih Tzye Kok ("Y.T. Kok"), and Samuel Chia ("Chia"), who joined Hytera and subsequently worked on Hytera's competing DMR products.

The parties agreed that at the time they left Motorola to join Hytera, G.S. Kok was a Senior Engineering Manager, Y.T. Kok was a Senior Software Engineer, and Sam Chia was an Engineering Section Manager. Dkt. 895. Motorola alleged that given their senior positions at the time, each of them worked on developing DMR products for Motorola and worked extensively with Motorola's proprietary and confidential information related to MotoTRBO products. Dkt. 435. Despite each signing two Non-Disclosure Agreements ("NDA") that specifically prohibited disclosure of any confidential information of Motorola—one as part of Motorola's Employment Agreement and the other as part of their exit materials—Motorola alleged that each of them secretly accessed and downloaded thousands of Motorola's confidential technical documents that contained Motorola's trade secrets shortly before their departure from Motorola in 2008, including Motorola's source code for its DMR products, and that these trade secrets were later incorporated into Hytera's products and business strategies. Dkt. 435.

In addition to the downloading of Motorola's confidential information, Motorola alleged that one of these individuals, Y.T. Kok, started working for Hytera on June 10, 2008 even before his official departure from Motorola on October 3, 2008, and that he downloaded, copied, and/or transmitted Motorola documents at some point during this

almost four-month period of double employment. Dkt. 878. As for Sam Chia, Motorola alleged that he spent a day at Hytera while still employed at Motorola and met with G.S. Kok, before downloading a massive amount of documents. Dkt. 878.

Motorola's Trial Strategy

The case was bitterly contested, as evidenced by the more than nine hundred docket entries, numerous motions to compel, multiple extensions of the case schedule, and the voluminous documents produced. After two and a half years, the case finally proceeded to a trial before an Illinois jury. The trial was an unusually lengthy one—the jury heard evidence and arguments on November 6, 7, 12-14, 18-21, 25-27, 2019, December 2-5, 9-12, 16-19, 2019, January 13, 21-23, 27-29, and February 3-5, 10-14, 2020.

Motorola's trial strategy was to tell the jury a story about a competitor company building its business on valuable proprietary information stolen from it, through (1) damaging internal communications from the defendants, (2) key individuals' refusals to answer questions based on their constitutional rights against self-incrimination, and (3) circumstantial evidence and testimony suggesting potential evidence destruction by the defendants. In support of its punitive damages claim, Motorola focused, among other things, on the alleged involvement of Hytera's senior management members in the misappropriation scheme and again, the alleged intentional destruction of relevant evidence.

At trial, Motorola presented evidence that Hytera used more than 10,000 confidential technical documents and millions of lines of source code that had been lifted from Motorola's databases. Further, documents produced by Hytera containing internal communications between Hytera employees, including the former Motorola Employees, showed concerns about "using a lot of Moto[rola's] code" and the need to "re-write softwares [sic] to look different from Motorola." There was also another Hytera document created by Sam Chia on August 1, 2008 stating that "[O]ption 2 is the best...[it] also had a low chance of detection if the code was dissembled by Moto[rola]." Dkt. 435.

The jury was also permitted (although not required) to draw adverse inferences based on the fact that G.S. Kok, Y.T. Kok, and Sam Chia declined to answer dozens of questions concerning how they shared Motorola's confidential information with other Hytera employees and the involvement of other senior managers at the company with the theft, citing their Fifth Amendment right to decline to respond to questions that could incriminate them. The jury was also allowed to draw adverse inferences from the fact that Peiyi Huang and Sam Chia "lost" three laptops that undisputedly contained thousands of confidential Motorola documents and source code files. Dkt. 878. Motorola further pointed out that "Hytera's expert Mr. Grimmett admitted that Hytera employees 'either deleted the records of [using Motorola's RAF concept document] or they went to a lot of trouble to make sure there wasn't a record showing how they were passing these things back and forth.'" Dkt. 827.

To support its punitive damages claim at trial, Motorola argued that Hytera engaged in "willful and malicious misappropriation" of trade secrets, which included "an intentional misappropriation as well as a misappropriation resulting from the conscious disregard of the rights of another." Dkt. 878. Motorola alleged that Hytera's President and CEO Mr. Chen—along with multiple Hytera engineers—knew of and participated in the misappropriation of Motorola's trade secrets, and Hytera then "attempted to cover up the theft by intentionally destroying evidence, including Motorola source code and documents." Dkt. 878. Motorola further argued that "Hytera is vicariously liable for the misappropriation of its employees and agents" because "Hytera ratified and approved of G.S. Kok, Y.T. Kok, Sam Chia, and Peiyi Huang's conduct by retaining the benefit of the misappropriation and continuing to sell the accused products that admittedly have Motorola's source code in them, attempting to delete or failing to produce evidence of the theft, and denying Motorola's claims through this litigation—until trial started in November 2019." Dkt. 878.

Hytera's Key Defenses at Trial

Hytera mounted several defenses in this case. Dkt. 762. For example, although Hytera did not deny that the former Motorola employees stole confidential documents from the plaintiff, during trial it rejected Motorola's claim that the improperly obtained information had spread beyond those individuals and disputed the significance of the information to the development of Hytera's products. Hytera argued before the jury that Motorola was attempting to hold the entire company responsible for the bad acts of only a few employees and intentionally delayed bringing the case in order to reap a large profit from Hytera's commercial success.[2] Hytera's lawyer was quoted as arguing that Motorola "want every single dollar that Hytera has earned" from the sales of its radios "going back to 2010, plus more."[3]

Another key issue in this case is that, in view of Motorola's significant damages claims, Hytera moved during trial to "preclude Motorola from relying on extraterritorial damages." Dkt. 834. This was a legal issue to be decided by the Court. Although the Court agreed with Hytera that the Illinois Trade Secrets Act does not have extraterritorial reach, it ruled in favor of Motorola that the federal Defend Trade Secrets Act can apply extraterritorially if the requirements of 18 U.S.C. § 1837 are met and that Motorola was entitled to recover damages flowing from exploitation abroad of the domestic acts of copyright infringement committed by Defendants. Dkt. 834.

The Jury Instructions and Verdict

While Motorola also claimed copyright infringement, the core of its case was based on alleged trade secret misappropriation. As explained in the jury instructions in this case, Motorola claimed trade secret misappropriation under both the Illinois Trade Secrets Act ("ITSA") and the federal Defend Trade Secrets Act ("DTSA"), which share several common elements. Under the Illinois Trade Secrets Act, in order to establish a claim for misappropriation of trade secrets, Motorola has the burden of proving: (1) Motorola owned the information at issue; (2) the information at issue is a trade secret; (3) the information at issue was misappropriated by Hytera in Illinois; and (4) the information was used by Hytera in its business. Similarly, under the federal Defend Trade Secrets Act, in order to establish a claim for misappropriation of a trade secret, Motorola has the burden of proving: (1) Motorola owned the information at issue; (2) the information at issue is a trade secret; (3) the information at issue was misappropriated by Hytera; and (4) the trade secret is related to a product used in, or intended for use in, interstate or foreign commerce. Dkt. 895.

Further, both the ITSA and DTSA make available exemplary/punitive damages in an amount not more than twice the amount of the compensatory damages if the misappropriation is "willful and malicious." According to the jury instructions, the jury was to assess exemplary damages only if it found that Hytera's conduct was malicious or in reckless disregard of Motorola's rights. Dkt. 895. Specifically, Hytera's conduct would be "malicious if it is accompanied by ill will or spite, or it is done for the purpose of injuring Motorola" and Hytera's conduct is "in reckless disregard of Motorola's rights if, under the circumstances, it reflects complete indifference to Motorola's rights, and not simply that Hytera was aware that the information was a trade secret." Dkt. 895.

After instructions and closing arguments by Motorola and Hytera, the jury started its deliberations. As noted above, the jury deliberated for only a little more than two hours before rendering its unanimous verdict, finding Hytera liable for trade secret misappropriation and copyright infringement and awarded Motorola the maximum it sought, $345.8 million in compensatory damages and $418.8 million in punitive damages, for a total of $764.6 million. The short deliberation by the jury in combination with the substantial damages award suggest that the jurors found Motorola's evidence at trial overwhelming. However, during trial, both sides moved for judgment as a matter of law which the Court took under advisement. In other words, Hytera in particular argued that the evidence presented by Motorola was insufficient and the case should not have gone to a jury verdict.

2 https://www.law360.com/articles/1246323/motorola-rival-could-see-global-ban-after-764m-radio-trial
3 https://www.bloomberg.com/news/articles/2019-11-07/motorola-claims-hytera-had-double-agent-steal-its-trade-secrets

Advice for Chinese Companies

This case suggests many lessons to be learned and practical considerations for Chinese technology companies:

1. EMPLOYEE HIRING AND TRAINING.

Given the front-and-center role of the activities of former Motorola employees in this case, companies should pay extra attention to the hiring process and regular training of new employees, especially those hired from a competitor. It is common nowadays to include provisions in both the employment agreement and the employee's handbook prohibiting the new hire from using any confidential and/or propriety information from his/her prior employer or any other third parties. But companies should not stop there. Technology companies in particular should also implement regular training programs emphasizing an employee's confidentiality obligation to all former and current employers to protect its confidential and/or propriety information and reduce or eliminate potential exposure to third party claims.

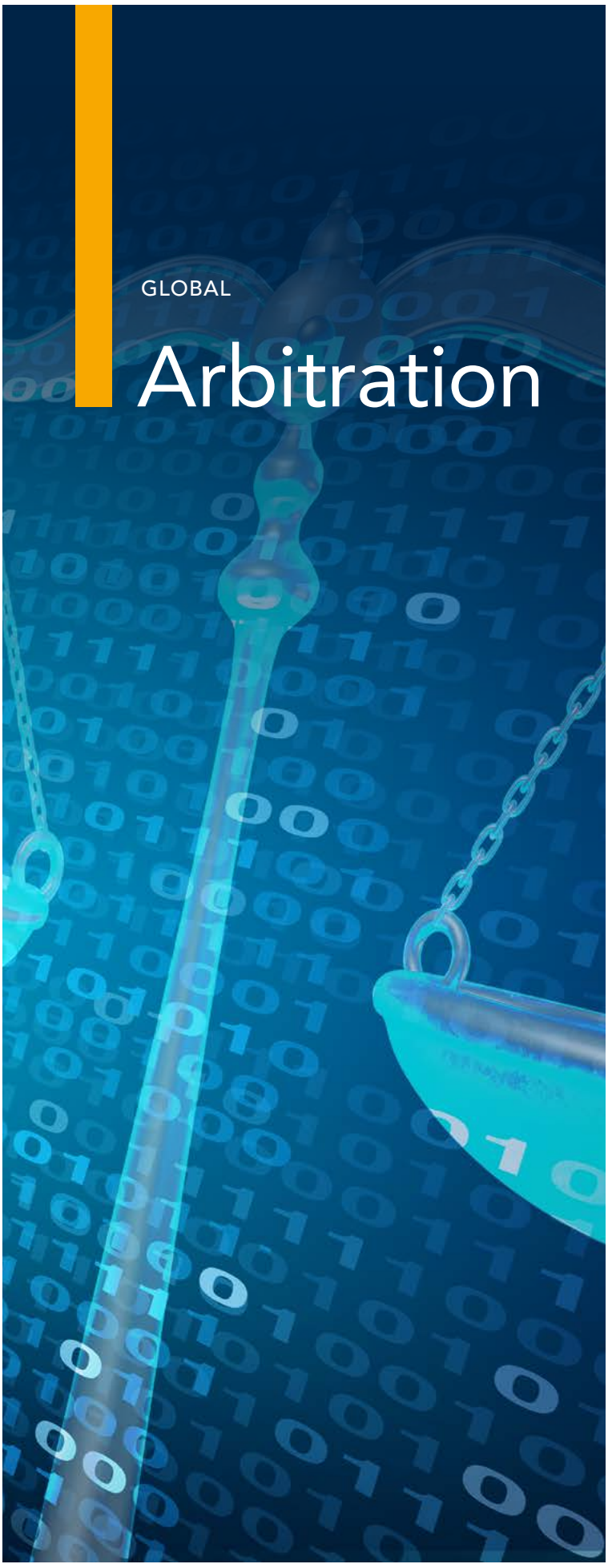
If the company discovers any misappropriation or misuse of any third party trade secrets or proprietary information by an employee, it should immediately contact the legal department or outside counsel to evaluate its options to remedy the situation. Any failure to take appropriate remedial measures can potentially lead to claims that the employer ratified or approved the employee's wrongful acts.

2. PRESERVATION OF DOCUMENTS AND FILES.

The failure to preserve potentially relevant documents can be extremely damaging to a party's position in U.S. litigation. Even inadvertent deletion or destruction of evidence might give rise to adverse inferences that the deleted or destroyed evidence would have been harmful to a party's position. As soon as litigation begins, or even the possibility of a claim arises, steps should be taken to ensure relevant evidence is not lost or destroyed. Litigation holds are routinely sent out by counsel during a pending litigation or sometimes in anticipation of a potential litigation to ensure that all employees who may possess relevant evidence are aware of their obligations. It is paramount for all company personnel to follow the instructions in the litigation hold and make sure that any potentially discoverable materials are preserved.

3. EXTRATERRITORIAL REACH OF DEFEND TRADE SECRETS ACT AND THE COPYRIGHT ACT.

In view of the Illinois Court's holding that the DTSA and the Copyright Act may allow a plaintiff to recover damages for extraterritorial acts that occur outside of the United States, Chinese companies with U.S. subsidiaries or commercial activities in the U.S. should be mindful of potentially broadened damages exposure. On the other hand, the extraterritorial reach of these statues could be extremely valuable for a Chinese company seeking to enforce its rights under these statutes through litigation in the U.S. courts.



Arbitration Update: the 2021 ICC Rules

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

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

On 6 October 2020, the International Chamber of Commerce ("**ICC**") Executive Board formally adopted the 2021 ICC Rules of Arbitration ("**2021 ICC Rules**"). The 2021 ICC Rules will come into force and apply to all arbitrations submitted to the ICC International Court of Arbitration ("**Court of Arbitration**") from 1 January 2021. Until then, the text of the 2021 ICC Rules available on the ICC's website is subject to editorial changes.

While the new 2021 ICC Rules do not represent a major shift in approach compared to the previous 2012 and 2017 ICC Rules, they contain a significant number of amendments and new provisions, which are seen by many as a welcome improvement, giving the ICC arbitral procedures more efficiency and flexibility.

Key Changes in the 2021 ICC Rules

JOINDER AND CONSOLIDATION

The 2021 ICC Rules add a new Article 7(5) in relation to a party's request to join an additional party to the arbitration ("**Request for Joinder**") *after* the confirmation or appointment of any arbitrator. The new article removes the existing requirement under the 2017 ICC Rules for all parties (including the additional party) to consent to the Request for Joinder, and only requires that the additional party consents to the composition of the arbitral tribunal and agrees to the Terms of Reference.

In deciding whether to grant the Request for Joinder, the arbitral tribunal has the discretion to take into account "all relevant circumstances", which may include: (i) whether the tribunal has *prima facie* jurisdiction over the additional party; (ii) the timing of the Request for Joinder; (iii) any possible conflicts of interest; and (iv) the impact of the joinder on the arbitral procedure.

In relation to consolidation of more than two or more arbitration proceedings, Article 10 of the 2021 ICC Rules now clarifies an issue as to whether consolidation of arbitration proceedings is only permitted when the claims arise out of the same arbitration agreement. The revised Article 10 permits consolidation of two or more arbitration proceedings: where (i) different parties are involved, but the claims are made under the same arbitration agreement or agreements; or (ii) the claims are not made under the same arbitration agreement or agreements, but the arbitrations are between the same parties, and the disputes in the arbitrations arise in connection with the same legal relationship and the Court of Arbitration finds the arbitration agreements to be compatible.

Both the above revisions in the 2021 ICC Rules will likely benefit complex arbitration proceedings involving multiple parties and contracts.

THIRD PARTY FUNDING AND CONFLICTS OF INTERESTS

In order to assist the arbitrators to comply with their duties regarding independence and impartiality, new Article 11(7) of the 2021 ICC Rules requires the parties to reveal the existence and identity of any third party which has entered into an arrangement for the funding of claims or defences and under which it has an economic interest in the outcome of the arbitration. While the new rule is in line with the existing approach of the Court of Arbitration as confirmed in the *ICC's Note to Parties and Arbitral Tribunals on the Conduct of Arbitration under the ICC Rules of Arbitration* dated 1 January 2019 (Paragraph 28)[4], it takes the existing approach further by imposing on the parties an express obligation to disclose relevant funding arrangements.

Further, the 2021 ICC Rules expands the power of the arbitral tribunal to "take any measure necessary to avoid a conflict of interest of an arbitrator arising from a change in party representation" under new Article 17(2). The arbitral tribunal will have the discretionary power to exclude a new party's representatives "in whole or in part" after considering the parties' written submissions on this point. This new rule may be viewed as an intrusion on a party's freedom to select legal representatives.

APPOINTMENT OF ARBITRATORS

New Article 12(9) of the 2021 ICC Rules provides that, notwithstanding any agreement by the parties on the method of constitution of the arbitral tribunal, the Court of Arbitration may, in exceptional circumstances, appoint the entire tribunal to "avoid a significant risk of unequal treatment and unfairness that may affect the validity of the award." This new rule may be a concern to parties who value the freedom to choose their arbitrator.

VIRTUAL HEARINGS

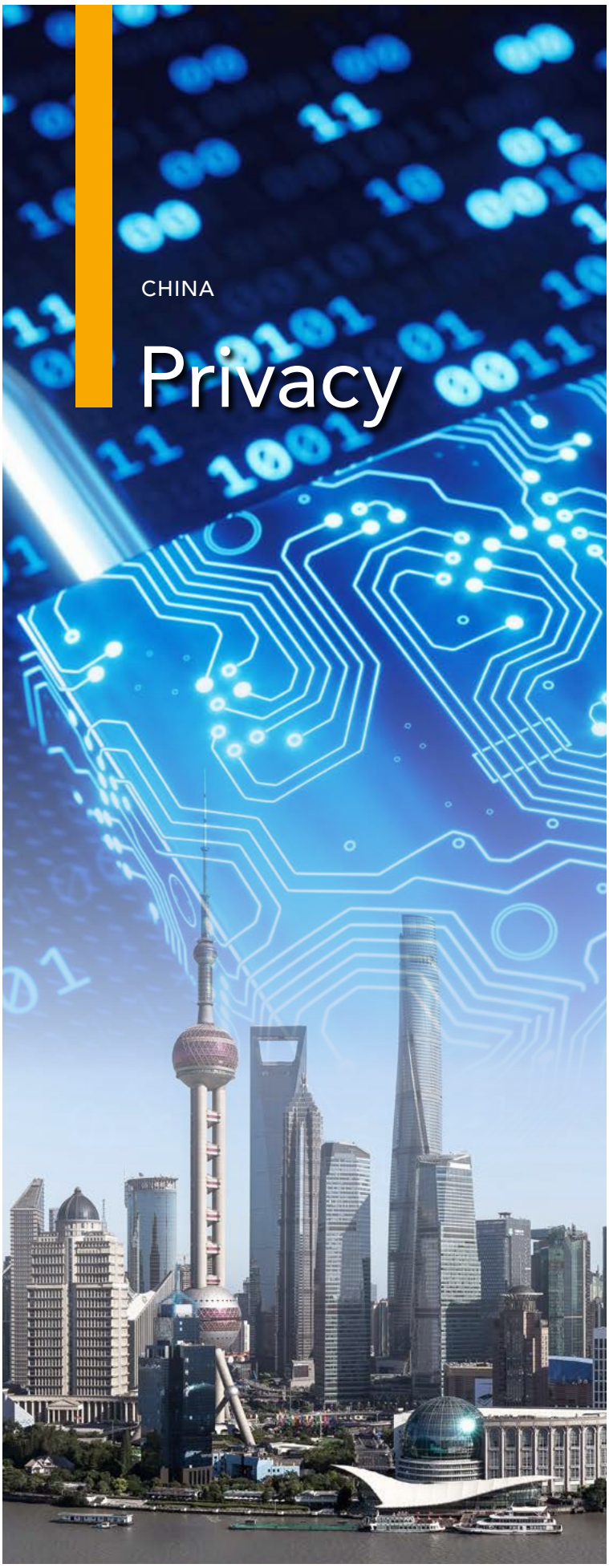
To accommodate the ever-evolving nature of how international arbitration is conducted, Article 26(1) of the 2021 ICC Rules gives the arbitral tribunal the discretion to decide whether a hearing should take place in-person or remotely by video conference, telephone or other appropriate means of communication, after consulting the parties and considering the relevant facts and circumstances of the arbitration.

Conclusion

The amendments and the new provisions in the 2021 ICC Rules are positive developments, providing the parties with greater flexibility and clarity on how the arbitration should be conducted. Nevertheless, some of the amendments, such as the arbitral tribunal's power to take any necessary measure to avoid a conflict of interest of an arbitrator arising from a change in party representation and the Court of Arbitration's power to appoint all the members to an arbitral tribunal, may add an element of uncertainty to the arbitration. Parties are encouraged to carefully review the applicable procedural rules of different arbitral institutions when entering into an arbitration agreement.

*The authors would like to thank **Douglas Yang**, Trainee Solicitor at Mayer Brown, for his assistance with this article.*

4 https://iccwbo.org/content/uploads/sites/3/2017/03/icc-note-to-parties-and-arbitral-tribunals-on-the-conduct-of-arbitration.pdf



Now It's Personal! China Issues Draft Personal Information Protection Law

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

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

On 21 October 2020, China's long awaited draft Personal Information Protection Law ("**Draft PIPL**") was released for public consultation.

Currently, China does not have an overarching data privacy law, and instead adopts a piecemeal approach to the protection of personal information, through laws such as the Cybersecurity Law and regulations and standards such as the Information Technology – Personal Information Security Specification. Once enacted, the Personal Information Protection Law will represent the first comprehensive law protecting personal information in China. The Draft PIPL is largely consistent with the numerous laws, regulations and standards already in place that touch on data privacy, and provides a clarification of the existing regulations in this space.

As with many new data privacy laws introduced elsewhere over the last couple of years, parallels can be seen between the Draft PIPL and the EU's General Data Protection Regulation ("**GDPR**"). Since its enactment, the GDPR has been held as the high standard for data privacy, and many jurisdictions in Asia have sought to introduce or amend their existing laws to bring them in line with the GDPR. Whilst similarities can be seen between the Draft PIPL and the GDPR, there are still some

noticeable differences. We have highlighted below some of the key aspects of the Draft PIPL.

Scope of Application

The Draft PIPL applies to the processing of personal information of individuals in China (regardless of their nationality). Similar to the GDPR, personal information is defined quite broadly, and applies to any information recorded in any format, which relates to an identified or identifiable individual.

The Draft PIPL is expressly stated to have extra-territorial effect, and applies to any overseas entity or individual who processes the personal information of a data subject, for the purpose of providing goods or services or analysing or assessing the behaviour of data subjects in China, or any other circumstances prescribed under the laws or regulations of China. Such overseas organisations or individuals must appoint a local representative or establish an entity in China, who shall be responsible for handling personal information protection matters, and their contact details must be registered with the relevant local authority.

This is similar to the GDPR, which also has extra-territorial effect in relation to the processing of personal information of data subjects located in the EU (regardless of nationality) by overseas entities, who target data subjects by offering them goods or services or who monitor their behaviour in the EU. The Draft PIPL uses broader definitions and concepts then the GDPR, which means that the provisions of the proposed law could apply to all e-commerce platforms that provide international shipping, including to China, even where they are not specifically targeting Chinese consumers.

Data Controllers

All organisations and individuals that independently determine the purposes, methods and other issues concerning the collection, storage, use, processing, transmission, provision, publishing and other such activities related to personal information, are subject to the requirements under the Draft PIPL. Whilst the Draft PIPL refers to them as "personal information processors", they are essentially the equivalent of data controllers under the GDPR.

However, in contrast to the GDPR, the Draft PIPL does not directly impose obligations on any service provider or third party that is entrusted by the data controller to handle personal information (i.e. the equivalent of a data processor under the GDPR). At most, such data processors are only required under the Draft PIPL to process the personal information strictly in accordance with the relevant data processing agreement with the data controller, to delete or return the personal information once the agreement is fulfilled or terminated, and are prohibited from further sub-contracting the processing of the personal data, unless it obtains the data controller's consent.

Data Protection Principles

The Draft PIPL sets out a number of data protection principles which on the whole are similar to the data protection principles found in the GDPR and most Asian jurisdictions:

a. the personal information should only be collected by lawful and proper means, and handled for clear and reasonable purposes;

b. only the minimum amount of personal information necessary to fulfil the relevant purpose should be collected, used, processed, stored, etc.;

c. the personal information should not be used for any unrelated purpose, unless the data subject's consent is obtained;

d. the personal information must be accurate and updated in a timely manner;

e. the principles of openness and transparency must be observed;

f. necessary measures must be implemented to safeguard the security of the personal information; and

g. no organisation or individual may handle personal information in breach of any laws or regulations, or in any manner that harms national security or the public interest.

Right to Process

In general, data controllers shall only be able to collect, process, use or otherwise handle personal information, if:

a. they obtain the data subject's consent;

b. it is necessary to conclude or fulfil a contract with the data subject;

c. it is necessary to perform obligations or to fulfil

any duties imposed under laws or regulations;

d. it is necessary in order to address any public health incident, or to protect an individual's life or health, or the security of their property in an emergency situation;

e. it is for the purpose of news reporting, supervising public opinion or other such activities that are in the public interest, and the use of the personal information is within a reasonable scope; or

f. any other circumstances provided under any law or regulation.

The Draft PIPL extends the legal basis on which data controllers can process personal information (under China's Cybersecurity Law, the only way in which organisations could process personal information was if they obtained consent). Whilst this is more in line with the GDPR, it does not include the right to process personal information in order to protect the legitimate interests of the data controller.

Consent and Notification

Clarification has been provided under the Draft PIPL as to what amounts to valid consent. It must be a voluntary and explicit indication of the data subject's wishes, given with full knowledge. If the data controller knows, or should have known, that the personal information they are processing is the personal information of a minor (i.e. an individual who is less than 14 years of age), then they must obtain the consent of the data subject's guardian.

Unless an exemption applies, the data controller should clearly notify the data subject of the following, before they collect, use or process their personal information:

a. the data controller's identity and contact information;

b. the purpose for which, and the methods that will be used, to collect, process, store, provide or carry out any other related activity in relation to the personal information;

c. how the individual can exercise their right under the Draft PIPL; and

d. any other information required under any law or regulation to be notified to the data subject.

If any personal information will be provided by a data controller to a third party, they must also obtain the specific consent of the data subject and notify them of the identity and contact information of the third party, the methods and purpose of use and the categories of information that will be transferred.

Data controllers are not allowed to refuse to provide any products or services to a data subject on the basis that they refuse to provide their consent or have withdrawn their consent in relation to the processing of their personal data, except if such processing is necessary in order to provide such products or services. For example, an organisation cannot refuse to provide telecommunication services to a customer, merely because the customer refuses to consent to the use of their personal information for marketing purposes.

Sensitive Personal Information

The Draft PIPL has defined "sensitive personal information", as any personal information that, if leaked or illegally used, might cause discrimination against an individual, or endanger their personal safety or property, including any information relating to race, ethnicity, religious beliefs, biometric features, medical health, financial accounts, location tracking information and other information. This definition is broader then the equivalent definition in the GDPR, which limits sensitive personal information to specific categories of data (i.e. racial or ethnic origin, political opinions, genetic data, biometric data where processes to uniquely identify an individual, trade union membership, religious or philosophical beliefs, or data concerning health, sex life or sexual orientation), and does not include a catch all phrase of "any other information" that could cause discrimination or endanger personal safety or property. Whilst on the one hand, the definition under the Draft PIPL allows for flexibility and further protection for data subjects, it also creates uncertainty as to the scope of the data controller's obligations in relation to sensitive personal information.

Under the Draft PIPL, data controllers can only handle sensitive personal information if: (i) it is sufficiently necessary to fulfil a specific purpose; (ii) they notify the data subject of why it is necessary and the potential impact on the data subject; and (iii) their separate and specific consent is obtained.

Written consent should be obtained if required under any law or regulation.

An express provision is included in the Draft PIPL that states that if stricter restrictions or a requirement to obtain any government authorisation is imposed under any other law or regulation for the processing of sensitive personal information, then such obligations must also be complied with. This means, for example, that data controllers will still need to comply with the requirements under the draft Measures for Data Security Management (once brought into operation), which were issued in relation to China's Cybersecurity Law, in addition to any obligations under the Draft PIPL. The draft Measures require any network operator that collects sensitive personal information to comply with certain filing requirements with the relevant local authority in relation to how they handle the sensitive personal information, and they must also designate a person to be in charge over the security of the sensitive personal information.

Cross-border Transfer Restrictions

Not surprisingly, and keeping in line with China's Cybersecurity Law, the Draft PIPL has stringent requirements on the cross-border transfer of personal information.

A key aspect of the Draft PIPL is the expansion of the data localisation requirement. The Draft PIPL follows China's Cybersecurity Law and imposes a requirement to keep all personal information stored in China on critical information infrastructure ("**CII**") operators, but also extends this obligation to any data controller whose volume of personal information processed exceeds the threshold specified by the Cyberspace Administration of China ("**CAC**"). Such threshold has not yet been prescribed. If any CII operator or such data controller wishes to transfer personal information overseas, it will need to undergo an official security assessment conducted by the CAC.

All other data controllers are prohibited from transferring personal information outside of China, unless one of the following conditions are met:

a. they obtain a certification carried out by an accredited body designated by the CAC;
b. they enter into an agreement with the foreign recipient that sets out their respective rights and obligations, and ensures that the personal information will be protected to the same standard as that provided under the Draft PIPL; or
c. they comply with any other conditions provided under law or regulations or prescribed by the CAC.

Aside from the above, any cross-border transfer of personal data will also require the separate consent of the data subject, who must be notified of the identity and contact information of the overseas recipient, the purpose and method for processing the personal information, the categories of personal information being transferred, and the way in which the data subject can exercise their rights provided under the Draft PIPL. A prior risk assessment must also be conducted by the data controller in relation to the cross-border transfers. Records of the risk assessment and of the cross-border transfers must be retained for at least 3 years.

If any personal information needs to be transferred outside China for the purposes of assisting foreign law enforcement authorities or providing judicial assistance, approval needs to be obtained from the relevant Chinese authority. This is consistent with China's draft Data Security Law issued in July 2020.

Data Subject's Rights

Data subjects are granted the right to know, decide, limit and refuse the processing of their personal information (unless such processing is otherwise required under law or any regulations), and they can also withdraw their consent at any time. They also have the right to access, obtain a copy of and correct their personal information held by a data controller. Data controllers are also obligated to explain how they handle personal information, if so requested by a data subject, and to delete personal information once the agreed retention period has expired, the purpose for processing has been fulfilled, the data controller ceases to provide the relevant products or services, or the data subject rescinds their consent, and so on.

Whilst these rights are reminiscent of provisions under the GDPR, the right to data portability is absent. This could be due to the potential difficulties and costs in implementing any data portability requests.

Mandatory Data Breach Notification

The Draft PIPL introduces a mandatory notification system, in the event of a data breach. Data controllers must take immediate steps to rectify the breach and they must notify both the relevant local authority and the affected individuals. Unlike the GDPR, there is no specific time limit for notification under the Draft PIPL.

The data controller will not need to notify the affected individuals if they have taken steps to effectively avoid any potential harm arising from the breach, unless otherwise ordered by the relevant authority. This seems to suggest that notifications should be made to the relevant authority in the first place and that with the authority's sanction, notification to the affected individuals may not be necessary.

Consequences for Breach

Violations of the Draft PIPL can result in a fine of up to RMB 50 million or 5% of the data controller's annual revenue for the previous financial year. It is unclear whether the data controller's revenue will be calculated on a global basis, as is the case with the GDPR. Individuals are also granted the express right to seek compensation from data controllers.

Conclusion

Due to its broad extra-territorial scope, foreign companies will need to reassess their operations in relation to China, and carry our data privacy audits in order to ensure compliance with the law once it is enacted. The data localisation and cross-border transfer restrictions may prove to be the most challenging, depending on the threshold set by the CAC. Overall, the Draft PIPL is a step in the right direction and brings China's data protection laws in line with the EU and major jurisdictions in the Asia Pacific region.

Update on Myanmar's Trade Mark Registration Framework

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

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

Introduction

After years of anticipation, Myanmar finally implemented a new framework for trade mark registration and protection by enacting the Trade Mark Law (Law No. 3/2019) (the "**Trade Mark Law**") on 30 January 2019. The Trade Mark Law provides the legal basis for the establishment of a formal trade mark registration system and the creation of an official trade mark office within the new Myanmar Intellectual Property Department (the "**IPD**").

The soft opening of the new trade mark registration system commenced on 1 October 2020 to allow existing trade mark owners the opportunity to re-register their trade marks under the new system.

The Old Regime

Prior to enactment of the Trade Mark Law, there was no formal trade mark registration system in Myanmar. In order to obtain trade mark protection, trade mark owners were required to submit a "Declaration of Ownership" of their trade mark and register the Declaration with the Office of Registration and Deeds. After registration of the Declaration, many trade mark owners would also publish a Cautionary Notice in a local newspaper to notify the public of its ownership and use of their trade mark (the "**Old Regime**"). The Old Regime did not provide for substantive examination or

opposition of trade marks and was a "First-to-Use" system, meaning that brand owners seeking to enforce their trade marks would need to show first use in Myanmar.

The New Trade Mark Registration System

The new trade mark registration system created under the Trade Mark Law will completely supersede the Old Regime. Trade mark applications under the new system will be formally examined and can be opposed, in line with practices in other countries with established trade mark registration procedures. The new system will be a "First-to-File" system, under which the priority of a trade mark will be determined by the filing date, irrespective of whether a mark has been used commercially in Myanmar.

Trade Marks under the Old Regime

Existing trade marks registered under the Old Regime will not be automatically protected when the new Trade Mark Law comes into effect. The soft opening of the new trade mark registration began on 1 October 2020 to give brand owners with trade marks registered under the Old Regime an opportunity to re-register their marks under the new system. The soft opening is expected to last for six months, but the exact end date has yet to be announced. Once the soft opening period ends, the Trade Mark Law will come into full force and the new trade mark registration system will officially replace the Old Regime.

All trade marks filed within the soft opening period will have the same filing date, which will tentatively be the effective date of the Trade Mark Law. All registrations will be valid for 10 years from the filing date.

Applications for re-registration during the soft opening period can only be made through authorised agents approved by the IPD. The official filing fees for each stage of the registration process are yet to be announced.

What Actions Should Existing Trade Mark Owners Take?

Brand owners with trade marks registered under the Old Regime should prepare the following information and documents for re-registration under the new system during the soft opening period:

1. copy of the Declaration of Ownership recorded with the Office of Registration and Deeds;
2. clear specimen of the trade mark *(should correspond to the Declaration)*;
3. owner's name and address *(should correspond to the Declaration)*;
4. classes and list of goods and/or services under the Nice Classification *(should correspond to or be narrower in scope than the Declaration)*; and
5. description of colour claim (if applicable).

New Trade Marks

New trade marks that have not been used in Myanmar or registered under the Old Regime can only be filed after the soft opening period. The filing date of such trade marks will be their actual filing date.

Conclusion

As the soft opening of the new trade mark registration system is still at its early stages, a number of issues remain unresolved. While it remains unclear when the new trade mark registration system will officially come into effect, brand owners with existing trade marks under the Old Regime should prepare the required documents and information to re-register their marks during the soft opening period to preserve their position. Further updates will be forthcoming as details of the new system are finalised by the IPD.

*The authors would like to thank **Stephanie Yung**, Trainee Solicitor at Mayer Brown, for her assistance with this article.*

Contact Us

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

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

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

Jing Zhang
Partner
+1 202 263 3385
jzhang
@mayerbrown.com

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

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

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

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