Morgan Lewis

ASIA CHRONICLE

Welcome to the 10th edition of *Asia Chronicle*! In this issue we examine recent and significant legal developments in Asia and how they may impact domestic and global companies doing business in the region; key features of the Cybersecurity Bill passed in Singapore; key legal and regulatory developments last year in India; China's national standard for personal data protection; and the Singapore Court of Appeal's clarification of *Said v Butt*. Hong Kong office managing partner Maurice Hoo discusses our firm's growth in Asia and Singapore-based litigation partner Stephen Cheong shares his insights on managing arbitration proceedings across Asia. We also highlight key recent transactions in which we have been involved, together with some of the seminars and conferences in which our lawyers have recently engaged across Asia.

SINGAPORE: CYBERSECURITY BILL PASSED

On 5 February 2018, the Singapore Parliament passed the Cybersecurity Bill.

The draft Cybersecurity Bill was previously released for public consultation. On 13 November 2017, the Ministry of Communications and Information (MCI) and the Cyber Security Agency of Singapore (CSA) published their report on the feedback received from the public consultation exercise on the draft Cybersecurity Bill. Certain amendments were made to the draft Cybersecurity Bill to take into account the feedback from the public consultation.

On 8 January 2018, the Cybersecurity Bill was tabled in the Singapore Parliament for a first reading. The Cybersecurity Act seeks to, among other actions, establish a regime to prevent, manage, and respond to cybersecurity threats and incidents, regulate owners of critical information infrastructure (CII), and regulate cybersecurity service providers.

EDITION 10

TABLE OF CONTENTS

Singapore: Cybersecurity Bill Passed 1

Key Developments in the Indian Legal Landscape in 2017. 4

China Publishes National Standard for Personal Data Protection 6

Singapore Court of Appeal Clarifies *Said v Butt* Principle 9

Hong Kong Office Managing Partner Reflects on Firm's Substantial Growth in Asia. 11

Doing Business in Asia? Here's What You Need to Know About Arbitration in the Region. 12

Our Work Across the Region. 14

Recognition of Our Practices 15

Legal Community Engagement 15

www.morganlewis.com

Key Features of the Cybersecurity Act

- The Commissioner of Cybersecurity (the Commissioner) has broad powers to administer the Cybersecurity Act.
- The Commissioner has the power to designate a computer or computer system as a CII for a period of five years if the Commissioner is satisfied that: (i) such computer or computer system is necessary for the continuous delivery of an essential service, the loss or compromise of which would have a debilitating effect on the availability of the essential service in Singapore; and (ii) such computer or computer system is located wholly or partly in Singapore.
- CII owners are subject to various statutory duties, including but not limited to providing information, complying with written directions of the Commissioner, providing notifications of any change in ownership, reporting cybersecurity incidents, carrying out cybersecurity audits and risk assessments, and participating in cybersecurity exercises.
- The Commissioner has powers to investigate and prevent serious cybersecurity threats or incidents and may direct any person by written notice to carry out remedial measures, or to cease carrying on certain activities.
- Service providers providing managed security operations centre (SOC) monitoring services and penetration testing services are required to be licensed under the Cybersecurity Act.

Appointment of a Commissioner of Cybersecurity

The Commissioner has broad powers to, among others, oversee and promote the cybersecurity of computers and computer systems in Singapore; respond to cybersecurity incidents that threaten the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore; regulate owners of CII; and establish cybersecurity codes of practice and standards of performance for implementation by owners of CII.

Critical Information Infrastructure

Computer systems directly involved in the provision of essential services are termed CII. The Commissioner has the power to designate a computer or computer system as a CII if the Commissioner is satisfied that:

- such computer or computer system is necessary for the continuous delivery of an essential service, the loss or compromise of which will have a debilitating effect on the availability of the essential service in Singapore; and
- such computer or computer system is located wholly or partly in Singapore.

An 'essential service' is defined as any service essential to the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore and which is specified in the First Schedule of the Cybersecurity Act:

- Energy
  - Electricity generation, electricity transmission, or electricity distribution services
  - Services for the supply or transmission of natural gas for electricity generation
- Info-communications
  - Fixed telephony services
  - Mobile telephony services
- Water
  - Water supply services
  - Services relating to collection and treatment of used water
  - Services relating to management of storm water
- Healthcare
  - Acute hospital care services
  - Services relating to disease surveillance and responses
- Banking and Finance
  - Banking services, including cash withdrawal and deposits, corporate lending, treasury management, and payment services
  - Payments clearing and settlement services
  - Securities trading, clearing, settlement, and depository services
  - Derivatives trading, clearing, and settlement services
  - Services relating to maintenance of monetary and financial stability
  - Currency issuance
  - Services relating to cash management and payments for the government
- Security and Emergencies
  - Civil defence services
  - Police and security services
  - Immigration services
  - Registration services under the National Registration Act of Singapore
  - Prison security and rehabilitation services
- Aviation
  - Air navigation services
  - Airport passenger control and operations
  - Airport baggage and cargo handling operations
  - Aerodrome operations
  - Flight operations of aircraft

- Land Transport
  - Rapid transit systems operated under a licence granted under the Rapid Transit Systems Act of Singapore
  - Bus services operated under a bus service licence granted under the Bus Services Industry Act 2015 of Singapore
  - Monitoring and management of rapid transit systems operated under a licence granted under the Rapid Transit Systems Act of Singapore
  - Monitoring and management of bus services operated under a bus service licence granted under the Bus Services Industry Act of Singapore
  - Monitoring and management of road traffic
- Maritime
  - Monitoring and management of shipping traffic
  - Container terminal operations
  - General and bulk cargo terminal operations
  - Cruise and ferry passenger terminal operations
  - Pilotage, towage and water supply
  - Bunker supply
  - Salvage operations
  - Passenger ferry operations
- Government
  - Services related to the electronic delivery of government services to the public
  - Services related to the electronic processing of internal government functions
- Media
  - Services related to broadcasting of free-to-air television and radio
  - Services related to publication of newspapers
  - Security printing services

For the purposes of the Cybersecurity Act, "essential services" are limited to those services expressly set out in the First Schedule of the Cybersecurity Act.

The designation will be effective for a period of five years unless it is withdrawn by the Commissioner before the expiry of such period.

Notice of Designation

CII owners will be given an opportunity to submit representations or appeal against a CII designation. The Cybersecurity Act allows for a person who receives a notice of designation to request for the Commissioner to amend the notice and address it to another person who has effective control over the CII (the Controller) by evidencing that the recipient of the notice of designation is not able to comply with the relevant requirements of the Cybersecurity Act as such person has neither effective control over the CII's operations nor the ability or right to carry out changes to the CII, unlike the Controller. If the Commissioner addresses and sends an amended notice to the Controller, the Controller will be subject to the relevant requirements of the Cybersecurity Act during the period when the notice is in effect, as if the Controller were the CII owner.

Duties of CII Owners

The Cybersecurity Act defines the owner of a CII as the legal owner of the CII, and, where the CII is jointly owned by more than one person, includes every joint owner. This makes it clear that computer systems in the supply chain supporting the operation of a CII will not (by virtue of supporting the CII) themselves be designated as a CII and third-party vendors will therefore not be regarded as CII owners.

The owners of CII (whether from the public or private sector) are subject to various duties to ensure the cybersecurity of their CII, including but not limited to:

- complying with codes of practice and standards of performance;
- complying with the written directions of the Commissioner;
- informing the Commissioner of any change in beneficial or legal ownership of the CII no later than seven days after the change in ownership;
- reporting cybersecurity incidents in respect of the CII and establishing mechanisms and processes for the purposes of detecting cybersecurity threats and incidents in respect of the CII as set out in any applicable code of practice;
- conducting cybersecurity audits of the CII at least once every two years (or at such higher frequency as may be directed by the Commissioner) by an auditor approved or appointed by the Commissioner;
- conducting cybersecurity risk assessments of the CII at least once a year; and
- participating in cybersecurity exercises.

A CII owner who does not comply with the provisions relating to regular cybersecurity audits and risk assessments may be guilty of an offence and shall be liable on conviction to a fine not exceeding S$100,000 or to two years' imprisonment or to both. The knowledge of an officer, employee or agent of a corporation may also be imputed to a corporation, and an officer, member or management of a corporation who consented to effect, or is party to, the commission of an offence under the Cybersecurity Act may also be found guilty of that same offence as the corporation.

Disclosure of Information

CII owners are required to furnish information relating to the CII to the Commissioner, including in relation to the design, configuration and security of the CII. Under the Cybersecurity Act, a person who is requested by the Commissioner to provide information does not have to do

so if such information is subject to any right, privilege or immunity conferred, or obligation or limitation imposed, by or under any law or rules of professional conduct in relation to the disclosure of such information (but note that performance of a contractual obligation is not an excuse for not disclosing the requested information). It is also provided in the Cybersecurity Act that a CII owner will not be treated as being in breach of any contractual obligation for doing or omitting to do any act, if the act is done or omitted to be done with reasonable care and in good faith and for the purpose of complying with a notice requesting for information.

Investigatory Powers

The Commissioner has powers to investigate and prevent serious cybersecurity threats or incidents and may direct any person by written notice to carry out such remedial measures, or to cease carrying on such activities, in relation to a computer or computer system which the incident response officer has reasonable cause to suspect is or was affected by the cybersecurity incident in order to minimize cybersecurity vulnerabilities in the computer or computer system.

Licensing Framework

Only providers of managed SOC monitoring services and penetration testing services are required to be licensed under the Cybersecurity Act. These service providers are required to be licensed on the basis that they have access to sensitive information from their clients, which could include the Singapore government and statutory boards. These services are widely used in the Singapore market, and hence have a significant impact on the overall cybersecurity landscape in Singapore.

Closing Remarks

The Cybersecurity Act is part of Singapore's broader cybersecurity strategy to safeguard essential services from disruptions by cyber-attacks and prevent and respond to cybersecurity threats and incidents. In formulating the Cybersecurity Act, the MCI and CSA studied cybersecurity legislation which other countries such as Germany, Estonia, the United States, Thailand and Vietnam have implemented or are considering to accord with international developments. It is also expected that specific codes of practice will be issued to provide guidance on the actions required to be compliant with the Cybersecurity Act.

The CSA has indicated that it will adopt a deliberate process in the designation of CII across different sectors, in consultation with owners and relevant sector regulators where possible. The CSA will implement programmes to help sector regulators assist CII owners in getting themselves ready to fulfil their obligations under the Cybersecurity Act. For example, schemes and awards have recently been set up to allow national servicemen in Singapore to attend cybersecurity professional courses and attain industry certifications.

Potential CII owners and members of the cybersecurity industry should take note of the provisions of the Cybersecurity Act. Organisations whose computers or computer systems are designated as CII will be notified in writing. If you are providing an 'essential service' in Singapore and have been, or are likely to be, designated as a CII owner, you may wish to consider your upcoming obligations under the Cybersecurity Act, which may require you to implement added cybersecurity measures, such as setting up network perimeter defence devices such as firewalls, or performing regular vulnerability scanning of computer systems to identify potential loopholes.

Contacts
Wai Ming Yap and **Gina Ng**

KEY DEVELOPMENTS IN THE INDIAN LEGAL LANDSCAPE IN 2017

In this article, we describe briefly what we consider to be some of the key legal and regulatory developments that India witnessed in 2017.

Right to Privacy: a Fundamental Right

In a landmark decision of *Justice K.S. Puttaswamy (Retd.) v Union of India and Ors*[1], the Supreme Court of India recognised the right to privacy as a fundamental right guaranteed by the Indian constitution. The Supreme Court held that the right to privacy is part of the right to life and personal liberty under Article 21 of the Constitution and part of the other fundamental rights contained in part III of the Constitution. The right to privacy being recognised as a constitutional right makes it an inviolable right as against the state and instrumentalities of the state. As against non-state actors, privacy is a common law right. In terms of statutory protection, the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (Rules) framed under the Information Technology Act, 2000 provide for the protection of sensitive data and personal information. India does not have a specific law on data protection; however, the government of India is expected to introduce such a law to address the subject matter in greater detail, as opposed to the current framework under the Rules.

Changes to Foreign Direct Investment (FDI) Policy

Under the 2017 the foreign direct investment (FDI) policy, a company or a limited liability partnership (LLP) having

[1] WP (CP) No. 494 of 2012

FDI is permitted to convert into an LLP and company respectively provided it operates in sectors where 100% FDI is permitted under the automatic route (i.e., no prior government approval required) and there are no FDI linked performance requirements under the automatic route. FDI was liberalised in certain sectors such as defence, pharmaceuticals and broadcasting. In the defence sector, 100% FDI is now permitted, with 49% being permitted under the automatic route and beyond 49% is permitted under the government route (i.e. prior government approval is required) when such further investments would result in access to modern technology in India or for certain other reasons. In the pharmaceutical sector, 100% FDI is now permitted in brownfield projects, where up to 74% FDI is permitted under the automatic route and beyond 74% is permitted under the government route subject to certain conditions. In the broadcasting sector, 100% FDI is now permitted under the automatic route. Under the 2017 FDI policy, there is no longer a requirement for prior approval from the Reserve Bank of India (RBI) for the establishment of a branch office, liaison office or project office, if the main business of the entity setting up such an office is related to information and broadcasting, telecom, private security or defence, and the required approval or permission from the relevant regulator or ministry has been obtained.

New Platform for Sexual Harassment Complaints

In a year that saw global outrage against sexual harassment, the Ministry of Women and Child Development (MWC) launched an online platform whereby female employees and visitors can raise complaints against sexual harassment at the workplace, be it in the private or public sector. The facility is named **SHe-box** (sexual harassment electronic box) and is aimed at providing an efficient redressal mechanism for the victim. Upon receipt of a complaint via the platform, the MWC will direct the complaint to the relevant employer's internal complaints committee or to the local complaints committee for further inquiry. The inquiry conducted by the relevant committee will also be monitored by the MWC. The introduction of this new facility is an indication of the government's strong view on the implementation of the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013.

Labour and Employment Law Reforms

The Indian government has been vocal in its desire to simplify and reform the labour laws. In its attempt to do so, 2017 saw many changes to labour regulations. The introduction in Parliament of the Payment of Gratuity (Amendment) Bill, 2017, (the Bill) has been approved by the Union Cabinet. The Bill seeks to increase the upper ceiling on payment of gratuity under the Payment of Gratuity Act, 1972, (PGA) from the current limit of INR 1,000,000 to INR 2,000,000. The PGA is a social security legislation that provides certain benefits to employees which are payable when the employee leaves the organisation. Enhancement of the wage ceiling has also been made under the Payment of Wages Act, 1936 (PWA). The PWA is a labour statute that provides for the payment of wages and related matter to workers in certain industries. The wage ceiling has been enhanced from INR 18,000 per month to INR 24,000 per month. This change will increase the number of employees covered under the PWA. The government has also introduced the Labour Code on Wages Bill, 2015, in the lower house of Parliament. This bill seeks to simplify and consolidate four critical pieces of legislation namely, the PWA, Minimum Wages Act, 1984, Payment of Bonus Act, 1965, and the Equal Remuneration Act, 1976. A significant reform has been the amendment to the Maternity Benefit Act, 1961, which has increased the duration of paid maternity leave from 12 weeks to 26 weeks. In addition to providing benefits to adoptive and commissioning mothers, the amendment also provides for an option to "work from home" after the expiry of the aforementioned 26-week period and it requires employers employing more than 50 women to provide crèche facility for its employees.

Changes to Foreign Investment Regime

The RBI replaced the Foreign Exchange Management (Transfer and Issue of Security by a Person Resident Outside India) Regulations, 2000, with the Foreign Exchange Management (Transfer and Issue of Security by a Person Resident Outside India) Regulations, 2017 (2017 Regulations). The 2017 Regulations overhaul the earlier regulations in so far as it clarifies a wide range of issues and ambiguities that existed under the earlier regulations. Under the 2017 Regulations, it is now clear that foreign venture capital investors are permitted to invest in non-convertible instruments and only listed companies can issue warrants to non-resident persons. Further, transfer of instruments by a non-resident Indian to a non-resident person does not require approval from the RBI. The 2017 Regulations states that delays in making filings such as Form FCGPR and Form FCTRS in respect of share issuance or transfer will not affect the title to the underlying securities but will only attract late fees as may be decided by the RBI.

New Trade Mark Rules

The Trade Mark Rules, 2002, have been repealed and replaced by the Trade Mark Rules, 2017. The new rules have reduced the number of forms/applications from more than 70 forms to just eight forms and these forms/ applications have also been simplified. A claim of 'prior use' is now being made more stringent with the requirement of relevant supporting documents including an affidavit. The registration process for a trade mark application has been expedited. Making an application for well-known marks is not possible, subject to the production of necessary supporting documents and following the processes, as set out by the guidelines issued by the Controller General of Patents, Designs and Trade Marks.

Company Law and Ministry of Corporate Affairs (MCA)

The MCA has notified Section 234 of the Companies Act, 2013 (2013 Act), which deals with cross-border mergers. Following this notification, company law in India now permits cross-border mergers where a foreign company merges into an Indian company and where an Indian company merges into a foreign company (incorporated in a specified jurisdiction). Prior to this, only a merger of a foreign company with an Indian company was permitted. The MCA has also notified additional exemptions under the 2013 Act for private companies and startups. Some of these include doing away of the requirement for quarterly board meetings for startups and interested directors will not be included in determining quorum for board meetings of private companies and startups, provided that their interest is duly disclosed to the board. The 2013 Act seeks to regulate the number of layers of subsidiaries through which investments can be made by companies. In connection with this, the MCA notified the Companies (restriction on number of layers) Rules, 2017, which sets out the category of companies which are not permitted to have more than two layers of subsidiaries. All companies other than banking companies, nonbanking financial companies considered systemically important, insurance companies, and government companies are restricted from having more than two layers of subsidiaries. This restriction is to only apply prospectively, and accordingly, all existing companies that have more than two layers of subsidiaries will not be affected by the notified rules. Going forward, companies will need to be mindful of these requirements when structuring their business.

Competition Law

Under the Competition Act, 2002 (2002 Act), parties to a combination were required to file a notification with the Competition Commission of India (CCI) within 30 days of the execution of the trigger documents. Failure in doing so attracted a penalty of up to 1% of, the higher of, the total assets or turnover of the combination. Following an amendment to this requirement, parties to a combination are exempt from making such a filing within 30 days and this exemption is available for a period of five years (i.e. until 29 June 2022). Structural changes to the institutions under the 2002 Act also took place, with the Competition Appellate Tribunal (COMPAT) being made redundant. The COMPAT was the appellant body for all appeals from the orders of the CCI. This function has now been transferred to the National Company Law Tribunal.

The year 2017 saw many significant and substantive changes to law and is in keeping with the current government's aim to reform laws to create a conducive and investor-friendly business environment in India.

Contacts:
Singapore | **Suet-Fern Lee** and **Anu Liza Jose**
Palo Alto | **Rahul Kapoor**

CHINA PUBLISHES NATIONAL STANDARD FOR PERSONAL DATA PROTECTION

With increased concerns regarding the safety of individual personal information, the Chinese government has clarified its existing data privacy rules regarding the collection, processing, and usage of personal data. Organisations operating in China should reexamine their data privacy policies in order to take into account the national standard for personal data protection, effective 1 May 2018, which provides detailed guidance for corporations to establish and maintain information governance systems.

With the development of information technology, collecting personal information has become a common business practice in Chinese commerce. But there have been many highly publicised cases of data abuse and leaks in recent years that have affected many industries, including education, healthcare, ecommerce, and telecommunications. The frequency, scale, and consequences of these incidents have made people increasingly concerned about the safety of their personal information. Businesses are also concerned about potential risk exposure in relation to customer data protection. Under these circumstances, the Chinese government decided to clarify some ambiguities in existing data privacy rules, especially in terms of the collection, processing, usage, sharing, transfer, and storage of personal data.

On 22 August 2016, the Office of the Central Leading Group for Cyberspace Affairs; the General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China (AQSIQ); and the Standardization Administration of the People's Republic of China (SAC) jointly issued Several Opinions on Strengthening National Cybersecurity Standardization Work (the Opinions). In Section II, 'Strengthening the Standardization Work,' the Opinions mentioned 'proceeding with the promulgation of the urgently needed standard,' and explicitly listed the 'personal data protection standard' as a focus of the government's recent work. On 29 December 2017, the AQSIQ and the SAC published a national standard for personal information protection: the Information Security Technology—Personal Information Security Specification (the Specification), which will be implemented on 1 May 2018. The Specification is a result of the national standardization efforts endorsed by the Chinese government. The entities involved in its drafting included government entities, universities, research institutions, and leading internet companies such as Tencent and Alibaba. From this perspective, unlike China's existing data privacy rules, which contain mainly abstract principles, the Specification is more practical and user-friendly, providing detailed guidance for corporations in terms of the establishment and maintenance of an information governance system.

As a 'technical guideline,' the Specification is at the third, and lowest, level of national standards and is not legally binding. However, according to the Opinions, the Chinese government considers the standardization 'an important component in the establishment of China's cybersecurity system,' and the Specification is intended to play a 'fundamental, normative, and guiding' role in China's cyberspace governance. As such, given the 'voice from the top' nature of the Specification, this standard is highly regarded and widely used despite the fact that it is not legally binding. The Specification has recently been cited by governmental authorities as the basis for some administrative decisions, such as a recent audit of the Cyberspace Administration of China (CAC), where Alipay was required to rectify its data collection/processing practices. Many commentators believe that the Specification sets best practices for Chinese companies for building firmwide personal data protection mechanisms, and will be used as comparison criteria when auditing companies under China's existing data privacy rules, notably the 2017 Cybersecurity Law. Due to the importance of the Specification in China's data privacy policy system, as well as its potential implications for the authorities' enforcement actions, multinational companies operating in China should pay close attention to this national standard and review their China practices accordingly to ensure compliance.

Relationship with Existing Data Privacy Laws

The Specification is said to be formulated under the umbrella of China's existing data privacy legal regime that includes, among others, the 2017 Cybersecurity Law (CSL); the Decisions on Safeguarding Internet Safety and the Decisions on Strengthening Protection of Internet Data issued by the Standing Committee of the National People's Congress; Amendments (V), (VII), and (IX) to China's Criminal Law; and the Provisions on Protecting the Personal Information of Telecommunications and Internet Users. The Specification is a supplement to the existing rules, but does not go beyond the principles laid out in existing laws and regulations. After the Specification was issued, many commented that the requirements contemplated by the Specification were stricter than those of EU counterparts. For example, the EU General Data Protection Regulation (GDPR) exempts the consent requirement for data processing in six situations. Among others, one of the commonly used nonconsensual grounds for collecting and processing personal information is legitimate interests, i.e., the necessity for data processing of the data controller overrides the data protection interests of the data subjects. However, a corresponding concept has not been adopted in the Specification. In a public speech, a Chinese policymaker explained that this is because the CSL explicitly requires that network operators in China obtain the data subject's consent for collection, leaving blank on the exceptions; thus the Specification must stick to the scope of existing rules and not delve into areas on which the law is silent.

That being said, it appears that the Chinese policymaker tries to echo the international practices in the ambit of CSL. Taking the consent issue above as an example, though the Specification does not adopt the legitimate interest concept, the other nonconsensual grounds for data collection and processing under the Specification are largely analogous to the relevant grounds under the GDPR. To some extent, the scope of China's nonconsensual grounds is even broader. For example, the Specification lists the necessity for product troubleshooting and news reports as grounds for data collection, which is not covered in the GDPR. And regarding legitimate interests, arguably the exceptions in the Specification have already covered some of the commonly seen examples of legitimate interests, including the necessity to protect the data subject's personal property or other significant rights and the necessity to execute a contract.

Key Definitions: Personal Information and Sensitive Personal Information

Before the issuance of the Specification, China had an existing national standard relating to personal data protection: the Guideline for the Protection of Personal Information in Public and Commercial Service Information Systems (the 2013 Guideline). It seems that the Specification was promulgated on the basis of the 2013 Guideline, while replacing and enriching the 2013 Guideline in many aspects. Among others, the Specification maintains the divided methodology as to general personal information and 'sensitive' personal information, a concept adopted in the 2013 Guideline. As with the 2013 Guideline, different protection levels apply to these two categories (as discussed below). Notably, the definitions of general personal information and sensitive personal information are also updated in the Specification.

For personal information, the definition in the 2013 Guideline and other data privacy rules mainly refers to data that could 'identify' a person, such as name and ID number. However, under the Specification, the definition of personal data is now extended to data that can be 'linked' to one person. Specifically, once an individual is identified through 'identifiable' personal information, any other data generated by this person in his or her following activities, even that on its own cannot be used to identify a person, also constitutes personal information. This other personal data includes individual location, communications records, and individual browsing history. In an annex attached to the Specification, the policymaker lists various examples. It is noteworthy that an individual's address book, friend list, classification of friends, and hardware serial code—types of information that are not identifiable per se—are now explicitly defined as 'personal information' and subject to data protection. This change indicates the policymaker's efforts to respond to the imminent society concerns over personal data safety by extending the scope of protection. Previously, many

companies designed their data protection systems to only protect such identifiable personal data as ID card numbers, telephone numbers, IP addresses, etc.

With the Specification in place, the policy clarifies for the first time that the data 'linked' to an identified person also requires special treatment. Undoubtedly, such update places a new requirement on companies in terms of data protection compliance. For sensitive personal information, the Specification generally takes a risk-based approach in its definition. 'Sensitive personal information' is defined as 'any personal information which, if lost or misused, is capable of endangering persons or property, easily harming personal reputation and mental and physical health, or leading to discriminatory treatment.' On the face of the language, the policymaker defines the 'sensitive' information broadly. According to the Specification, examples of 'sensitive personal information' include individual identifiable information such as ID card number, IP address, financial information, healthcare information, sexual orientation, religion, unpublished criminal records, communication records, internet browsing history, GPS location, etc. In addition, the Specification enhances the protection of children as it generally provides that all information regarding children younger than 14 years old is sensitive personal information.

Application Scope

The Specification applies to the Information Controller, a new position combing the concept of the 'personal information administrator' and 'personal information receiver' in the 2013 Guideline. The Specification defines 'Information Controller' as any organisation or individual with the power to determine the purpose and method for processing personal information, including any private or public organizations. This is seemingly modeled on the 'data controller' concept under the GDPR.

Consent Requirement and Notification Obligation

The Specification generally follows the basic principle set by the 2013 Guideline and the CSL that the consent of the Information Subject must be obtained before personal information is collected or processed, but puts more emphasis on the notification obligation of an Information Controller. The following information must be conveyed to the Information Subject when collecting information:

Personal information: For personal information, (1) the purpose for which and the method by which personal information is collected and used, e.g., the frequency with which the information is collected, where and how long the information will be stored, and whether the information will be shared with or transferred to others; and (2) if an Information Controller indirectly collects personal information from a third party other than the Information Subject, the Information Controller must confirm with the third party that (i) the personal information is obtained from a legal source and (ii) the Information Subject has authorised the third party to disclose or transfer the personal information and the proposed use of the personal information does not exceed the scope agreed by the Information Subject; otherwise, the Information Controller must obtain explicit consent from the Information Subject.

Sensitive personal information: The Specification for the first time distinguishes the requirements for core and ancillary functions: (1) if the information is required for an Information Controller to provide core business functions, the Information Subject must be informed of the consequence if he or she refuses to provide the information; and (2) if the information is for ancillary functions, the Information Subject must be informed of the specific ancillary function that requires the information; if the Information Subject refuses to provide the information, the Information Controller may refuse to provide such ancillary functions. However, if the Information Controller has obtained the necessary information for core business functions but does not obtain the information for ancillary functions, the Information Controller cannot cease providing the core functions due to the lack of information for ancillary functions.

In general, before an Information Subject can use an online service, a privacy policy prepared by the company's Information Controller will be delivered to the Information Subject for consent. Previously there was no standard requirement for such policy, so the Information Controller tended to include provisions that expanded its rights to collect and process personal information. The Specification, for the first time, provides standardised content and suggested privacy policy language in order to restrict the Information Controller's use and disclosure of the personal information collected. For example, the policy must include whether and to what extent the Information Controller can disclose the personal information to a third party; how the Information Subject can access, modify, and delete the personal information collected; and how the Information Subject can make a complaint.

Rights of the Information Subject

Compared with the 2013 Guideline and the CSL, the Specification grants the Information Subject more control over the personal information collected. For example, the Information Subject has the right to (1) know what information has been collected and its purpose, and whether the information has been collected by any third party; (2) modify and delete the information provided; and (3) withdraw the consent provided.

Rights of the Information Subject

Compared with the 2013 Guideline and the CSL, the Specification grants the Information Subject more control over the personal information collected. For example, the Information Subject has the right to (1) know what information has been collected and its purpose, and whether

the information has been collected by any third party; (2) modify and delete the information provided; and (3) withdraw the consent provided.

Obligations of the Information Controller

The Specification further enhances the obligations of the Information Controller in terms of information transfer and security.

Under the Specification, additional obligations will arise if an Information Controller transfers personal information to a third party due to the following:

- Upon outsourcing of the personal information processing matters, the Information Controller must
  - ensure that the outsourcing arrangement is compliant with the prior consent granted by the Information Subject;
  - conduct risk assessments of the third party and ensure that the third party has sufficient capability in terms of data security;
  - supervise the third party, sign proper contracts and conduct audits;
  - accurately record the status of the outsourcing arrangement.
- Upon mergers, acquisitions, and reorganisations, the Information Controller must
  - notify the Information Subject that the Information Controller will undergo a change; and
  - ensure that the successors and assigns continue performing obligations after the change. In case of any change to the purpose of using personal information, the explicit consent from the Information Subject must be re-obtained.

The Specification also requires that the Information Controller enhance measures for data security in terms of the following:

- that the legal representative or other key management take the leading role for personal information security, including providing sufficient support to personnel and finance;
- Control of internal access to the information collected. Specifically, the Information Controller must (1) ensure that only the relevant internal staff have access to the personal information, and (2) establish internal approval procedures for important operations on the personal information.
- Company governance. The Specification requires, among other things,
  - that the legal representative or other key management take the leading role for personal information security, including providing sufficient support to personnel and finance;
  - the Information Controller appoint key personnel or a department responsible for information protection matters;
  - the Information Controller establish a system to regularly evaluate the security risk at least once a year;
  - the Information Controller execute confidentiality agreements with the personnel processing personal information and conduct background checks on them;
  - the Information Controller provide training regarding the processing of personal information at least once a year or when there is a significant change to the privacy policy; and
  - the Information Controller conduct audits on the privacy policy, relevant company policies, and security measures.

Conclusion

The release of the Specification shows that the Chinese government takes data privacy regulations seriously. Although the Specification is not mandatory, further laws and regulations may refer to the Specification for personal information protection. Therefore, we suggest that organisations operating in China reexamine their data privacy policies to make them compliant with the Specification. The Specification also leaves some areas blank for the development of further legislation, such as the cross-border transfer of personal information. We will continue to follow updates and will keep you posted.

Contact:
Todd Liao

SINGAPORE COURT OF APPEAL CLARIFIES *SAID V BUTT* PRINCIPLE

In the recent case of PT Sandipala Arthaputra v STMicroelectronics Asia Pacific Pte Ltd [2018] SGCA 17 (PT Sandipala v STMicroelectronics), the Singapore Court of Appeal (SGCA) was given the opportunity to clarify the scope of application of the *Said v Butt* principle in determining when a director would be held personally liable for directing his company's breach of contract with a third party. In the first modern-day elucidation of the principle, the SGCA held that a director would ordinarily be immune from liability in tort for authorising or procuring his company's breach of contract in his capacity as a director, unless his decision is made in breach of any of his personal legal duties to the company.

PT Sandipala v STMicroelectronics Background

In *PT Sandipala v STMicroelectronics*, PT Sandipala Arthaputra (Sandipala) contracted for 100 million microchips (Contract) from Oxel Systems Pte Ltd (Oxel). The microchips were to be manufactured by STMicroelectronics Asia Pacific Pte Ltd (ST-AP). Sandipala wanted to use the microchips in an electronic identification card project in Indonesia, but the microchips were incompatible for use. Therefore, Sandipala rejected delivery of a large portion of the chips and refused to pay for the chips.

Sandipala sued Oxel for breach of contract, fraudulent misrepresentation, and unlawful means conspiracy, among other things. Oxel counterclaimed against Sandipala for breach of the same contract. Oxel also claimed that Sandipala and its directors, Paulus Tannos and Catherine Tannos (the Tannoses), had engaged in unlawful means conspiracy.

In particular, Oxel counterclaimed against Sandipala and its directors for conspiracy to cause Oxel loss by unlawful means by attempting to unlawfully extricate Sandipala from its contractual obligations owed to Oxel under the Contract by bringing a false claim against Oxel, creating a false paper trial for this purpose, and causing to be published articles containing false allegations against Oxel.

The High Court dismissed Sandipala's claims and allowed Oxel's counterclaims. Sandipala and its two directors appealed the decision. On appeal, the SGCA only allowed Sandipala and the Tannoses' appeal in relation to the claim in unlawful means conspiracy. This meant that Sandipala was still liable for Oxel's losses from its Sandipala's breach of the Contract, but the Tannoses were not personally liable in conspiracy.

SGCA's Judgement on Said v Butt Principle

With regards to Oxel's counterclaim against Sandipala and its directors in unlawful means conspiracy, the SGCA considered the question: When should a director be held personally liable for the consequences arising from his company's breach of a contract with a third party, to which only the company, and not he himself, is party? (at [50])

The SGCA recognized three potential situations when a director may be held personally liable: (1) when the director induces the company to breach its contract with a third party, (2) when the directors conspire to procure their company to breach the contract, or (3) when the director and the company conspire to breach the contract (at [51]).

Under the *Said v Butt* principle, immunity will be granted if the director acts bona fide within the scope of his authority. However, as the authorities are unclear as to what it means to act "bona fide within the scope of his authority", the SGCA took this opportunity to clarify this.

The SGCA recognized that under the *Said v Butt* principle, two issues remained unclear. First, whether the phrase "bona fide within the scope of his authority" is made up of two conjunctive requirements. Second, whether this required the directors to act lawfully and/or whether this requirement relates to the director's relationship with the third party or with the company.

Earlier Singapore cases interpreted the *Said v Butt* principle to comprise of two conjunctive requirements: (a) acting bona fide; and (b) acting within the scope of the director's authority. It was considered that this phrase only applied to directors who genuinely and honestly endeavoured to act in the company's best interests. If these elements were satisfied, the director would be immune from liability notwithstanding that he may have been genuinely mistaken as to the company's contractual obligations or even that he had the predominant intention of causing loss to another.

On the other hand, the principle under English law is that a director could lose immunity if his act of inducement was in breach of the director's own contract with or legal duty owed toward the company, while Australian authorities considered that a director who exercised his function as director and acted within his authority would be immune to personal liability. Canadian cases held that a director would be immune if he acted bona fide within the scope of his authority in the best interests of the company. However, even if he did not do so, he would only be personally liable his dominant concern was on depriving the third party of its contractual benefits.

After examining the relevant authorities, the SGCA concluded that the *Said v Butt* principle should be interpreted to "**exempt directors from personal liability** for the contractual breaches of their company (whether through the tort of inducement of breach of contract or unlawful means conspiracy) **if their acts, in their capacity as directors, are not in themselves in breach of any fiduciary or other personal legal duties owed to the company**". Personal legal duties may include the director's fiduciary duty to act in the best interests of the company, or contractual duty toward the company to act within the scope of his authority as granted by the company. The SGCA held that the **relevant focus of the bona fide inquiry is vis-à-vis the company and not the third party**. Therefore, even if the director had acted with an intention to injure the third party (thus failing to act bona fide against the third party), he may still fall within the immunity afforded by the *Said v Butt* principle if he acted in the best interests of the company and not in breach of any other duties. The burden of proving that the directors have breached their personal legal duties to the company lies with the plaintiff claiming against the directors. This interpretation was held to be fair, favours commercial certainty and efficacy in the performance of a director's functions, and is in line with earlier cases.

In terms of Sandipala's breach of contract, the SGCA found that there was no conspiracy between Sandipala and its directors. The SGCA accepted Sandipala's argument that the High Court had erred in relying on acts occurring after

the breach of contract as acts in purported furtherance of the conspiracy. Further, the SGCA accepted that there was no evidence that the directors had acted in breach of their personal legal duties to the company. To the contrary, the directors had acted in the best interests of the company to breach the contract with Oxel. In light of this, the directors were entitled to immunity under the *Said v Butt* principle.

Given that *PT Sandipala v STMicroelectronics* is the first clear exposition on the *Said v Butt* principle, it is likely to be widely adopted in other Commonwealth countries, including the United Kingdom and Hong Kong. The clarification is a positive development for company directors, as it circumscribes the scope of a directors' personal liability for his company's breaches of contract and it is only where the directors act unlawfully vis-à-vis the company, that they will be held personally liable in tort for unlawful means conspiracy. Importantly, directors should note that the focus of the inquiry is on their conduct and intention in relation to the company and whether they had acted in the company's interests.

Contacts:
Daniel Chia and **Annette Liu**

HONG KONG OFFICE MANAGING PARTNER REFLECTS ON FIRM'S SUBSTANTIAL GROWTH IN ASIA

Last month, Morgan Lewis celebrated its first anniversary in Hong Kong, the firm's 30th office* worldwide. Over the past four years, the firm has expanded its presence in Beijing, Shanghai, Hong Kong, Tokyo, and Singapore with new locations and significant lateral hires.

Our offices across Asia are closely integrated with the rest of the firm globally, with each strategic opening and lateral hire deepening our ability to serve clients in cross-border business transactions and international disputes. In addition to focusing on the effective integration of our Asia-based colleagues, we continue to advise companies doing business across the region on complex cross-border M&A transactions, capital markets financing, private equity investments, investment management regulatory and transactional work, real estate, intellectual property protection, Foreign Corrupt Practices Act (FCPA) and corporate compliance, and litigation and arbitration disputes.

In this Q&A, Hong Kong office managing partner Maurice Hoo shares his thoughts on the firm's trajectory in Asia and what clients are watching.

How has Morgan Lewis grown recently in Asia?

One year ago, we established a presence in Hong Kong, giving us a world-class team of corporate lawyers not only in Hong Kong but also in Beijing and Shanghai. Capping off our concerted multi-year focus on Asia, this step resulted in a tremendous expansion of our practices in this critical part of the world.

Our Hong Kong team has grown further in the last year and has established itself as a driving force in our global capital markets, corporate, and private equity practices. In addition to the corporate team that first joined a year ago, the Hong Kong office has since added a dispute resolution team, which is handling litigation in Hong Kong for our multinational clients headquartered in the United States and elsewhere, and an investment management team. Our growth in Hong Kong is reflected in our exciting recent move into a brand-new office in the financial heart of Hong Kong's business district.

The opening of the Hong Kong office came on the heels of significant expansion in China in 2016, when Morgan Lewis added a team of more than 25 legal professionals in Shanghai, greatly expanding our capabilities in M&A, private equity, real estate, fund formation, FCPA, and international disputes. In 2015, the firm secured a key base of operations in the thriving business center of Singapore with its novel combination with the Stamford Law Firm, which was the first law firm in the city-state to fully integrate with a global law firm. The successful merger produced a transactional, litigation, and arbitration powerhouse with the ability to practice across all legal service areas in Singapore and across Southeast Asia. And in 2014, we significantly grew our Tokyo office with the addition of a leading asset management practice, giving us a market-leading investment management practice in Japan.

With so many large groups arriving, how has Morgan Lewis made sure that effective collaboration is at the core of this growth?

As we grow, our shared commitment to collaborate across the firm has enabled us to succeed exponentially. Integrating the Stamford group; our new colleagues in Beijing, Shanghai, and Hong Kong; and new lawyers in every office while improving client service and operational excellence has required successful collaboration at a very high level. Over the last year, we have had three meetings bringing together all of our Asia partners with the full leadership of the firm, and our associates have been involved in integration programs in both Asia and the United States.

Our practices are led globally and work together daily across borders. In addition, our integration has been accelerated by the firm's focus on industry groups, which are vital to the representation of global clients. Bringing together lawyers across practices and geographies that really understand a specific industry brings incredible value to our clients' businesses and creates natural working groups among our lawyers. And that collaborative approach is also what has allowed us to broaden and deepen our relationships with our clients.

Last summer, BTI Consulting Group named Morgan Lewis one of three firms with the "best collaboration." We see this play out every day as our partners in Asia are leading or supporting key cross-border matters for clients across the firm. We can now assist global clients in nearly every area where they might have a challenge or opportunity in Asia, in addition to advising Asia-based clients facing issues globally—from intellectual property to investment management to complex litigation to global antitrust issues.

What kind of work is the Hong Kong office handling for clients?

Since joining the firm, our Hong Kong corporate team—working together with Beijing and Shanghai teams and colleagues globally—has completed more than 65 private equity transactions with an aggregate deal value exceeding $4.4 billion; executed more than 50 cross-border M&A transactions, collaborating with numerous offices worldwide in inbound and outbound transactions; closed multiple IPOs in a diverse set of industries ranging from education, utilities, and construction, to automobiles and components; and collaborated extensively with our Singapore colleagues in dual listings on the Hong Kong and Singapore exchanges.

In what ways is Morgan Lewis making a commitment to Asia?

Success in the highly competitive, complex, and fast-evolving Asia legal market requires well-integrated teams of elite lawyers, not simply a presence in the region. Like many of our most successful global clients in a diverse set of industries, we marry teamwork with proficiency, international perspectives with local practices, and firm commitment with personal grit. It is not a market for law firms (or any business for that matter) to dabble in, but with the strength and collaborative culture of our firm, we are in an excellent position to build in this market and serve our clients well.

Is Morgan Lewis planning further expansion in the region?

Our growth is driven by what our clients need and where they need us to be. It is obvious from the volume of work our Asia offices are already engaged in with multinational companies that markets in Asia are key components of their own growth strategies, so I expect it will continue to be for us as well.

** Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners.*

DOING BUSINESS IN ASIA? HERE'S WHAT YOU NEED TO KNOW ABOUT ARBITRATION IN THE REGION

The popularity of international arbitration as a preferred dispute resolution mechanism in Asia, reflecting ongoing engagement in cross-border investment across and from outside the region, has resulted in the continued development and refinement of national arbitral rules and laws across many of these jurisdictions.

While arbitration rules and procedures will often have common features globally, it is important to remember that cultural, geographical, and commercial differences still have a significant impact on the conduct of arbitration around the world, and must be considered carefully at the contract drafting stage before deciding whether to arbitrate, where to arbitrate, and which procedural rules to adopt in resolving any dispute.

Morgan Lewis partner Stephen Cheong, a disputes partner in the firm's Singapore office, lays out some of the key reasons companies involved in cross-border investment choose arbitration as the mechanism by which commercial disputes will be resolved and some of the key things to be aware of when arbitrating in Asia. For more detailed information, please see the second edition of ***An Introductory Guide to Arbitration in Asia***, which covers key elements of the arbitration frameworks in 14 key jurisdictions that have continued to attract significant investment activity. The guide addresses commonly asked questions that global businesses should consider in connection with international arbitration proceedings in these jurisdictions and the enforcement of arbitral awards across Asia.

Why would companies involved in cross-border deals choose arbitration over litigation?

For many years, a significant proportion of contracting parties have chosen arbitration over litigation based on a number of factors: the arbitration may be conducted confidentially in a neutral venue, rather than publicly in the state of either contracting party; the parties can select a tribunal that is familiar with their industry sector and the course of dealing within that sector; and a procedural timetable can be agreed upon that provides a clear way forward to the hearing and the award, enabling the parties to budget for the time and cost of resolving their dispute. Grounds for appeal are often limited and the award itself can be enforced directly in more than 150 countries through the New York Arbitration Convention on the Recognition and Enforcement of Foreign Arbitral Awards, 1958.

Do you think this trend toward arbitration will continue to grow?

The continued popularity of arbitration as a dispute resolution mechanism is reflected in the growth of a number of international arbitration centers throughout Asia. In turn, arbitration centers have developed procedural rules that parties may adopt to govern the appointment of the tribunal and, subsequently, the procedure that parties may follow to resolve their disputes. At the same time, national arbitration laws across jurisdictions in Asia have been reviewed and refined to support the arbitration procedure in that jurisdiction and the enforcement of arbitration awards from overseas. A number of jurisdictions in the region have developed their arbitration institutions as a crucial element of their standing as part of a key global financial center.

What were some of the changes made to arbitral rules in the last year?

China, India, Thailand, and Vietnam all updated their arbitral rules in 2017. In China, the Arbitration Law came into effect 1 January 2018, and the People's Republic of China (PRC) Civil Procedure Law came into effect 1 July 2017, with both applying to domestic and international arbitration. Under the PRC's Civil Procedure Law, corporations waive their right to bring an action in people's court if an arbitration clause is included in an initial contract. The Arbitration Law further clarifies the scope of arbitration agreements, providing that an arbitration agreement must contain an intention to arbitrate, define the scope of disputes that are to be arbitrated, and identify the arbitration commission chosen by the parties to administer the arbitration. In India, the arbitration act does not in specific terms exclude any category of disputes—civil or commercial—from arbitration. However, an award will be set aside if the court finds that the subject matter of the dispute is not capable of settlement by arbitration under the laws currently in force, or if the award conflicts with Indian public policy. There is no appeal from arbitral awards made in India. A domestic award may only be set aside by the courts upon application by a party. Any such application must be made within three months from the date on which the party making the application received the arbitral award. In Thailand, foreign nationals may only represent clients in arbitration if the law governing the dispute is not Thai law or if the award will not be enforced in Thailand. And in Vietnam, the Civil Procedure Code came into effect 1 March 2017, and specifies that certain disputes, including civil cases related to immovable property, divorce proceedings involving a Vietnamese citizen and foreigner, and civil cases where the parties have the right to select the jurisdiction of the Vietnamese courts, are subject to the exclusive jurisdiction of the Vietnamese courts and are therefore not arbitrable in Vietnam.

What are some best practices for companies when reviewing arbitration agreements?

Some of the main points to be considered when drafting and negotiating an arbitration agreement in Asia include the following:

- Define the scope of the agreement to arbitrate to make sure it is broad enough to cover all anticipated disputes and claims and clear enough to avoid any potential jurisdiction challenges. It is also helpful to determine what language everyone is comfortable using to avoid the need for interpreters.
- Determine the seat and venue of the arbitration, as the seat of the arbitration usually determines the law that governs the arbitration (if not already specified in the arbitration agreement). For example, if the seat of the arbitration is Singapore, then the legal position governing applications for injunctive relief before the arbitral tribunal will be governed by Singapore law. Parties should select a place that is neutral and where the national courts are supportive of arbitration.
- Decide who will administer the arbitration. Parties can decide to have the arbitration administered by a recognised arbitral institution (e.g., SIAC, HKIAC, LCIA) or administered in accordance with their own set of agreed procedures (i.e., ad hoc arbitration). While more costly than ad hoc arbitration, the arbitral institution can assist in matters such as securing the appointment of the arbitrators, setting and administering the arbitrators' fees (which may be scaled based on the aggregate sum in dispute), supervising the arbitration, and reviewing the arbitral award. In an ad hoc arbitration, parties may save on the cost of appointing the arbitral institution to administer the arbitration but will have to determine all aspects of the arbitration themselves.
- Adopt rules of arbitration in the initial agreement. Differences exist between each of the popular institutional rules and it is recommended that parties consult with their lawyers when selecting a set of institutional rules that meets their needs.
- Determine the proper number of arbitrators: one or three. While appointing a sole arbitrator may be cheaper and potentially more efficient, a sole arbitrator may not have the legal and/or technical expertise to determine all issues in dispute.
- Specify the governing law of the contract and of the arbitration. The law that parties wish to apply to govern the disputes that arise should be identified in the arbitration agreement (if not identified elsewhere in the contract). Otherwise, it may be a source of dispute if parties from different countries insist that the laws of their respective countries should govern the contract from which the

dispute arises. Similarly, parties should specify the governing law of the arbitration and should not assume that the governing law of the arbitration follows the seat of the arbitration, the governing law of the contract, or the venue of the arbitration. Failing to specify the governing law of the arbitration may evolve into a preliminary issue that the arbitral tribunal will have to determine.

OUR WORK ACROSS THE REGION

From our offices across the region, and together with our colleagues globally, we continue to advise businesses based in and operating across Asia in connection with high-profile transactions and complex disputes. Key recent examples include:

Temasek Linked Fund to Invest in Ezion Holdings

We recently represented Singapore mainboard-listed offshore and marine operator Ezion Holdings in its issuance of shares and options to Pavilion Capital Fund Holdings, a Temasek linked fund. If all options are converted into shares, Ezion will raise up to S$50 million.

We have also been advising Ezion, which recently emerged from a months-long complex debt refinancing exercise having secured support from all classes of stakeholders. This is the first investment in Ezion by a strategic investor in the prolonged industry downturn. Ezion is the owner of one of the youngest, largest and most sophisticated fleets of multi-purpose self-propelled service rigs in the world and one of the first to promote the usage of multi-purpose self-propelled service rigs in Asia and the Middle East. Ezion is also the only operator in Southeast Asia with a fleet of service rigs that can be used in the offshore oil and gas industry as well as the offshore wind farm industry.

Led by Singapore corporate and business transactions partner Bernard Lui with substantial assistance from Singapore associates Jorina Chai and Jeremiah Huang.

Ezion Holdings Secures US$2.0 Billion Refinancing

Morgan Lewis represented Ezion Holdings Ltd. in securing almost US$2 billion in refinancing from its secured lenders and debt securityholders. The company has resumed trading in its shares after an eight-month suspension following the approval from the Singapore Exchange. This was after the receipt of approvals from shareholders for the issuance of the new shares, warrants and bonds according to the terms of its US$1.5 billion refinancing from secured lenders and US$420 million refinancing from holders of its various series of medium term notes and perpetual securities. We represented the company in the various milestones.

The refinancing undertaken by the offshore and marine services provider took almost nine months to complete and, particularly with respect to the consent solicitation in relation to the debt securities and the subsequent implementation, was the most complex and unprecedented in Singapore to date. The refinancing exercise involved multiple work streams in connection with its structuring and implementation, and its success required the team to ensure coordination among banks and other lenders, holders of multiple series of debt securities and the trustee of such securities, shareholders, equity investors, the Singapore Exchange and the clearing system.

Led by Singapore corporate and business transactions partner Bernard Lui and finance partner Sin Teck Lim, substantially supported by Singapore corporate and business transactions associates Jorina Chai and Yu Kwang Lui, and assisted by Singapore trainees Zi Liang Tan, Kristian Lee and Shawn Yeo.

Tikehau Investment Management: Formation of TKS I

We advised Tikehau Investment Management on the formation of its first healthcare-focused venture capital fund, TKS I LP. The fund will primarily invest in early-stage companies in the healthcare or life sciences industry, including those looking to commercialize the application of artificial intelligence and the digitization of healthcare. The fund held its first closing on 4 January and Tikehau plans to raise up to $75 million in commitments from investors in Singapore, the United States, and other jurisdictions.

Led by Singapore investment management partner Daniel Yong with assistance from Singapore associate Si Ning Teng. Advice on US law was provided by investment management partner Charles Horn (Washington, DC), and associates Omar Hemady (Boston) and Miranda Lindl O'Connell (San Francisco); tax of counsel Gabe Quihuis (Boston); and EB/EC partner Craig Bitman (New York) and associate Chris Payne-Tsoupros (Washington, DC).

Shun Tak: Investment in Perennial HC Holdings

We recently represented Shun Tak Holdings Ltd. in its investment in a consortium to invest up to US$1.2 billion in healthcare-related property projects in China. The consortium is sponsored by Singapore Exchange–listed Perennial Real Estate Holdings Ltd. The joint venture vehicle, Perennial HC Holdings Pte. Ltd., will invest in, acquire, and develop healthcare-integrated, mixed-use developments connected to high-speed railway stations in mainland China. With a 30% stake in the joint venture vehicle and an initial first tranche commitment of US$150 million, Shun Tak will be the second-largest consortium member. Perennial Real Estate and Shun Tak will also jointly establish asset, project, and hotel management companies to manage the

developments. Shun Tak's participation in this joint venture will allow it to expand and diversify its property investment portfolio into the healthcare industry in China.

Shun Tak is a leading conglomerate with core businesses in the property, transportation, hospitality, and investment sectors, and is listed on the Stock Exchange of Hong Kong. We previously represented Shun Tak when it invested in another Perennial-led consortium to acquire TripleOne Somerset, an office and retail development project in Singapore, for S$970 million (US$734.8 million).

Led by investment management partner Daniel Yong (Singapore) with assistance from associate Si Ning Teng (Singapore).

RECOGNITION OF OUR PRACTICES

China Business Law Journal: Firm Recognized in 3 Practice Areas

Morgan Lewis has been named among the top law firms in three practice categories by the *China Business Law Journal* as part of its China Business Law Awards series for 2017. We earned the distinction in the Education, Employment and Labor, and Intellectual Property (Patent and Trade Secret) categories. The awards are based on hundreds of nominations and comments received mostly from China-focused corporate counsel, senior managers, and legal professionals around the world, as well as each firm's landmark deals, cases, and other notable achievements in the last year.

Amarjit Kaur Named to Singapore's 'Most Promising Legal Luminaries'

Singapore litigation associate Amarjit Kaur was recognized by *Singapore Business Review* on its list of "Singapore's most promising legal luminaries aged 40 and under." The list honors 20 Singapore lawyers aged 40 or under for their thought leadership, influence, and success over the last year. The honorees were selected from hundreds of nominees with specializations ranging from disputes resolution and litigation, mergers and acquisitions, finance, and construction to intellectual property, copyright, media law, family law, and energy.

Singapore Office Contributes to Law Society's Advocates for the Arts

Our Singapore office recently completed a pro bono project for the Pro Bono Services Office of the Law Society of Singapore. Our team made contributions to the organisation's legal handbook, Advocates for the Arts, which aims to contextualise and explain legal issues relevant to the creative arts industry to safeguard its members from common exploitative practices such as nonpayment. We drafted two chapters in the handbook, "Contracts 101" and "Insurance." The Law Society's Pro Bono Services Office recognised our significant contributions to the book by awarding certificates of appreciation to the firm and contributors Singapore corporate and business transactions partner Joo Khin Ng and litigation associate Amarjit Kaur.

LEGAL COMMUNITY ENGAGEMENT

Our lawyers across Asia, in conjunction with colleagues globally, continue to engage with the legal community across the region through conferences and seminars covering a range of commercial law issues. Key recent examples include the following. We would be pleased to discuss how Morgan Lewis can offer similar educational insight to your business.

Morgan Lewis Presents at China Intellectual Property Roundtable 2018

Intellectual property partner Shaobin Zhu (Shanghai) presented "Recent Development of IP Enforcement in China" and intellectual property partner Bob Busby (Washington, DC) presented "The Landscape in US IP Litigation for Chinese Companies" at the China Intellectual Property Roundtable 2018 held by Global Intelligence Communications on 17 April in Shanghai. Intellectual property associate Chris Liu (Shanghai) and corporate and business transactions associate Sabrina He (Shanghai) also attended the conference.

Shaobin Zhu Presents on Chinese Companies Doing Business Overseas

Shanghai intellectual property partner Shaobin Zhu presented "Recent Trends of Legal Risks for Chinese Companies Doing Business Overseas" on 31 March at the China Corporate Counsel 30-People Forum—Chinese Enterprises "Going Out" Seminar in Qingdao. The event was co-sponsored by firm client Haier and the Association of China Corporate Counsel, with Legal Daily, a legal affairs newspaper supervised by China's Ministry of Justice.

Morgan Lewis Co-Sponsors Seminars in China with CACLO

On 23 and 24 March, Morgan Lewis co-sponsored seminars in Hangzhou and Shenzhen with the China Academy of Chief Legal Officer (CACLO) titled "IP Protection and Compliance Forum" and "US Patent Deployment and Litigation Strategy Salon," respectively. Intellectual property practice leader Eric Kraeutler (Philadelphia) provided a "US Patent Litigation Update"; partner Shaobin Zhu (Shanghai) presented on "How to Minimize IP Risks in View of Recent

Lawsuits Against Chinese Companies"; and partner Bob Gaybrick (Washington) spoke about "Settlement Strategies in View of a Changing IP Environment" in both Hangzhou and Shenzhen. During the program in Hangzhou, the IP team was joined by litigation partner Chris Warren-Smith (London), who presented on "Global and Cross-Border Compliance & Investigations" and labour and employment practice partner Sarah Bouchard (Philadelphia), who presented on "Navigating Workplace Harassment Issues in the #MeToo Era."

The seminars had a strong turnout with more than 50 attendees in Hangzhou and more than 100 in Shenzhen.

From left are intellectual property partners Shaobin Zhu (Shanghai) and Eric Kraeutler (Philadelphia); corporate and business transactions China advisor Agatha Zuo (Shanghai); and intellectual property partner Bob Gaybrick (Washington) and associate Chris Liu (Shanghai).

Morgan Lewis Launches WeChat Corporate Account in China

Morgan Lewis launched a WeChat corporate account in China, which shares information about our firm's capabilities, news, insights, activities, and thought leadership. Known as China's "super app," WeChat has become an essential social-media business tool for people working and living in China. Please scan the QR code to follow us on WeChat!

Singapore Office Hosts Crisis Management Seminar for Clients

Our firm recently hosted a seminar in our Singapore office called "Bridging the Legal-PR Divide in a Crisis-Driven World," presented by litigation partners Gordon Cooney (Philadelphia) and Chris Warren-Smith (London), and Stamford corporate services director Elaine Lim (Singapore). The seminar discussed the great divide between legal and communications considerations in managing crises, and offered guiding principles for finding common ground and successfuly collaborating to achieve crisis mitigation and

Client representatives attend "Bridging the Legal-PR Divide in a Crisis-Driven World" in our Singapore office.

Singapore Office Hosts Corporate Governance and Compliance Seminar

Morgan Lewis recently presented a seminar, "Hot Topics and Trends: Capital Markets, Corporate Governance, and Securities Compliance Matters," in our Singapore office. The seminar discussed the latest trends and emerging themes relating to corporate governance and securities compliance, and provided insight into stockholder activism, US Securities and Exchange Commission initiatives, risk management, and stockholder governance litigation. Corporate and business transactions partners Bernard Lui (Singapore), Timothy Corbett (London), Joanne Soslow (Philadelphia), Laurie Cerveny (Boston), and Wai Ming Yap (Singapore), and finance partner Sin Teck Lim (Singapore) presented at the event.

Representatives from current and prospective clients attend the seminar in our Singapore office.

Singapore Office Conducts M&A Seminar

Corporate and business transactions partners Steve Browne (Boston), Charlie Engros (New York), David Pollak (New York), Bernard Lui (Singapore), and Wai Ming Yap (Singapore) recently presented a seminar, "The Devil Is in the Details: Mergers & Acquisitions," in our Singapore office. The seminar discussed global trends in M&A and overlooked areas in transactions that can cause issues, including cross-

border deals; M&A insurance; the Committee on Foreign Investment in the United States; regulatory clearances and timings; central-bank capital controls; tax advice; stakeholders' approvals; and local jurisdiction requirements, culture, or country-specific documents.

From left are corporate and business transactions partners Steve Browne (Boston), Charlie Engros (New York), David Pollak (New York), and Wai Ming Yap (Singapore) during the recent seminar in our Singapore office.

Singapore Office Hosts Seminar on Navigating Workplace Harassment Issues

Labour and employment partner Grace Speights (Washington, DC) and litigation partner Daniel Chia (Singapore), and associate Amarjit Kaur (Singapore) hosted a seminar on "Navigating Workplace Harassment Issues in the #MeToo Era" on 19 March in our Singapore office. The seminar addressed the changing landscape of workplace harassment in the pre- and post-#MeToo era. The discussion focused on ways companies can get ahead of potential issues, including by conducting cultural assessments and putting in place anti-harassment policies and reporting/investigation protocols.

Firm Publishes Second Edition of *Guide to International Arbitration in Asia*

The popularity of international arbitration as a preferred dispute-resolution mechanism in Asia, reflecting ongoing engagement in cross-border investment across and from outside the region, has resulted in the continued development and refinement of national arbitral rules and laws across many of these jurisdictions. The second edition of Morgan Lewis's *Guide to International Arbitration in Asia* covers the key elements of the arbitration frameworks in 14 key jurisdictions which have continued to attract significant investment activity. The guide addresses commonly asked questions which global businesses should consider in connection with international arbitration proceedings in these jurisdictions and enforcement of arbitral awards across Asia. Along with Morgan Lewis partners Justyn Jagger and Stephen Cheong (Singapore), Charles Mo (Hong Kong), Tsugumichi Watanabe (Tokyo) and Mitch Dudek and Todd Liao (China), we received valuable input on some areas of local law and practice during the preparation of the Guide from firms in key jurisdictions across the region. Find the guide **here**.

Singapore Office Conducts PDPA Training and Networking Seminar

Corporate and business transactions partner Wai Ming Yap (Singapore) recently presented a seminar on the Personal Data Protection Act (PDPA) in our Singapore office. The training and networking seminar, co-hosted by Jason Tan, director at WAB Lab Pte. Ltd., explored the ways and means of how businesses from different industries can keep up with the latest trends in the data protection sphere. The seminar covered the latest developments in the PDPA, practical tips for implementing data protection best practices, and essential knowledge for data protection officers.

Litigation associates Amarjit Kaur (Singapore), Kenneth Kong (Singapore), and Yanguang Ker (Singapore) were also in attendance.

Participants in the recent training and networking seminar in our Singapore office.

Bernard Lui Presents at Listed Company Directors Programme

Corporate and business transactions partner Bernard Lui (Singapore) was a speaker at the Listed Company Directors Programme on 24 January at the Marina Mandarin Hotel in Singapore. Bernard presented on corporate governance during the "Understanding the Regulatory Environment in Singapore" seminar, discussing the roles and responsibilities of the board and individual directors, remuneration matters, accountability and audit considerations, shareholder rights and responsibilities, and regulatory updates. He also served as the panel moderator at the end of the session, which included the Singapore Exchange's head of listing compliance.

The Listed Company Directors Programme, organised by the Singapore Institute of Directors and supported by the Singapore Exchange, is a comprehensive, in-depth program focusing on the specific training needs of listed company

directors—in particular, the independent directors. The program is composed of six modules on the range of regulatory, compliance, and corporate governance matters of listed companies in Singapore.

US Tech M&A Client Seminar and Reception in Tokyo

Corporate and business transactions partners Nancy Yamaguchi (San Francisco) and Bradley K. Edmister (New York) and antitrust partner J. Clayton Everett, Jr. (Washington) gave a client seminar titled "Pitfalls in US Technology M&A and How Japanese Corporations Can Avoid Them" to 80 Japanese executives on 16 April in Tokyo. They covered Silicon Valley corporate, litigation and antitrust issues and obstacles that Japanese corporations especially face. Ms. Yamaguchi focused on the recent trends in Silicon Valley and technology markets in the United States overall and major pitfalls and how to avoid them touching on corporate, intellectual property, and employment law. Mr. Edmister provided detailed deal strategies and structures for acquisitions for public companies while Mr. Everett focused on litigation and antitrust issues in getting the deal through and explained features of the American litigation system for Japanese corporations in controlling litigation risk and limiting litigation cost.

Tsugu Watanabe, managing partner of our Tokyo office, welcomed our guests and introduced other US partners Alan Neuwirth (New York) and Satoru Murase (New York), and Tokyo partners Chris Wells, Tomoko Fuminaga, Tadao Horibe, and Carol Tsuchida.

Partners Nancy Yamaguchi (top), Bradley K. Edmister (middle), and J. Clayton Everett, Jr. (bottom) present to the US Tech M&A Client Seminar and Reception in Tokyo.

Morgan Lewis

CONTACTS

Suet-Fern Lee
Singapore
+65.6389.3030
suetfern.lee@morganlewis.com

Mitch Dudek
Shanghai
+86.21.8022.8788
mitch.dudek@morganlewis.com

Edwin Luk
Hong Kong
+852.3551.8661
edwin.luk@morganlewis.com

Christopher P. Wells
Tokyo
+81.3.4578.2533
chris.wells@morganlewis.com

Aset A. Shyngyssov
Almaty | Astana
+7.727.250.1005 | +7.7172.925.985
aset.shyngyssov@morganlewis.com

Maurice Hoo
Hong Kong
+852.3551.8551
maurice.hoo@morganlewis.com

Xiaowei Ye
Beijing | Shanghai
+86.10.5876.3689 | +86.21.8022.8588
xiaowei.ye@morganlewis.com

Ning Zhang
Hong Kong | Beijing
+852.3551.8690 | +86.10.5876.3586
ning.zhang@morganlewis.com

Daniel Yong
Singapore
+65.6389.3074
daniel.yong@morganlewis.com

Lynette Chew
Singapore
+65.6389.3067
lynette.chew@morganlewis.com

www.morganlewis.com