FULL REPORT FOR FRGS 16-006-0505

Legal Framework for Theft of trade secrets and Corporate Espionage in Malaysia: Adhering to the Trans Pacific Partnership Agreement (TPPA)

Keywords: Trade secrets, corporate espionage, TPPA, misappropriation

Project Leader: Dr. Juriah Abd Jalil

Researcher: Dr. DuryanaBinti Mohamed
Dr. Nasarudin Bin Abdul Rahman
Mr. Raja BadrolHisham Bin Raja Mohd Ali
Dr. Halyani Hassan

Summary of Research

Misappropriation or theft of trade secrets and corporate espionage threaten innovation, growth, development and investment of business entities and national economy globally. Civil remedies alone are insufficient to protect trade secrets from these growing threats. As a measure to address this issue, the Trans-Pacific Partnership Agreement (TPPA) requires signatory countries to criminalize theft of trade secrets and corporate espionage. In Malaysia, the common law of breach of confidence, and breach of contractual obligation particularly contract of employment provides remedies to the owner of the trade secret against misappropriation. However, there is no specific statute to protect trade secrets from these threats under the civil and criminal law. As a signatory to TPPA, Malaysia has to adopt this provision into the national law within two years after the signing of the agreement. But what options do we have and which model should Malaysia adopt? This research seeks to examine the adequacy of the common law and to investigate the relevant civil, criminal and cyber laws in protecting trade secrets in Malaysia with the aim of providing recommendation on the establishment of a legal framework in line with the TPPA requirement. A benchmarking exercise with other signatories countries namely the United States, United Kingdom and Japan, will be conducted, apart from adopting a SWOT analysis of all relevant legislation policies and case law relating to protect of trade secrets in Malaysia. Focus Group Discussion and semi-structured interviews will be conducted to examine the impact of these threats in Malaysia. The outcome of this research will be a material source of reference

for the Malaysian government to establish a comprehensive legal framework in combating theft of trade secrets and corporate espionage as compliance to the TPPA requirement.

Problem Statement

Trade secret, as the most valuable intellectual property assets of a business is facing a threat from misappropriation, theft and corporate espionage. (OECD, 2015) The threat continues to rise particularly with the proliferation of digital devices, wireless technology competition within the industry and trans-border business. (US Chamber of Commerce, 2013). Technological developments such as digitization of business records, widespread use of portable electronic devices and cloud computing renders businesses more vulnerable to cyber theft of trade secret and cyber espionage (Seaman, 2015) The effect of this crime is tremendous since it undermines the company potential ability to further innovate, grow and invest in the markets. (CREATE, Feb 2014) It's also threatened the emerging markets and the growth of small business. (EC, 2013)

The issue in relation to the protection of trade secret is not new. It was addressed in the TRIPs Agreement requiring signatories to protect trade secret and confidential information under Art 39. The focus of TRIPS is on providing civil and commercial remedies. But recently the Trans Pacific Partnership Agreement (TPPA) where Malaysia is one of the partners requires signatory countries to impose criminal penalties for misappropriating or disclosing, willfully and without authority, trade secrets relating to a product in national or international commerce for purposes of commercial advantage or financial gain, and with the intent to injure the owner of such trade secret. The provision was proposed by the United States, Mexico, Canada, New Zealand and Japan but was opposed by Australia, Singapore, Malaysia, Peru, Vietnam, Chile and Brunei Darussalam. Nevertheless the agreement was signed on the 4th February 2016, thus Malaysia is obligated to incorporate this into her national laws within 2 years from this date.

At present, there is no statutory protection of trade secret in Malaysia. This far, misappropriation of trade secret and confidential information are protected under the common law of breach of confidence, breach of fiduciary duty and/or duty of fidelity and the law of contract particularly contract of employment. (Juriah, 2003) But this does not deter the theft of the company's trade secret particularly cyber theft and third party to continue threatening the development and existence of a business entity. In 2010, instances of divulging trade secrets and corporate

espionage has been discussed and highlighted in the Malaysian case of *Worldwide Rota SdnBhd v Ronald Ong CheowJoon* [2010] MLJU 288. The court rely on the law of breach of confidential information to find the defendant, a former employee who start a new similar business to be liable but the third person who committed the corporate espionage or acted as a spy for him was only called to be the witness. In the case of *Dibena Enterprise SdnBhd v Huawei Technologies (Malaysia) Sdnbhd& Anor* [2012] MLJU 154 the court considered the 1st defendant argument on the impact of commercial espionage on it business and other companies that have dealing with it, before limiting the plaintiff application for discovery of documents which contain sensitive commercial trade secret between the defendant, a company in Hong Kong and Telekom Malaysia Berhad. These two cases show that corporate espionage and theft of trade secrets have indeed occurred in Malaysia. But there is no specific criminal law addressing such act as crime. Therefore there is an urgent need for Malaysia to have a comprehensive legal framework to combat the growing threat of theft of trade secret and corporate espionage as support to the TPPA.

Hypothesis

The Malaysian legal framework should consist of robust civil remedies and effective criminal enforcement to curb the growing risks of theft of trade secret and corporate espionage.

Objective (s) of the Research

1) To examine the common law protection of trade secrets and safeguards in protecting the threat of misappropriation of trade secrets and corporate espionage in Malaysia;

2) To investigate and examine the relevant civil, criminal and cyber laws protecting trade secrets in Malaysia;

3) To conduct a bench marking exercise with other countries namely the United States, United Kingdom and Japan, signatories to the agreement;

4) To propose recommendation for an appropriate and effective legal framework for Malaysia.

Research Questions

1. Whether the present state of the common law and relevant civil and criminal law in Malaysia effective to combat theft of trade secret and corporate espionage?

2. Should Malaysia have a specific legislation governing both civil remedies and criminal liability to combat the risk of theft of trade secret and corporate espionage?

3. Whether taking of confidential corporate information by dishonest means for rival counterpart amount to criminal liability?

4. Whether there should be criminal liability for the deliberate misuse of trade secrets belonging to others?

5. Whether wrongful acquisition of trade secret and use it for personal gain amount to unfair competition under the Malaysian Competition thus invite criminal liability.

Literature Reviews

Protecting trade secrets is critical for the continued prosperity and economic security of business globally. The economist, in the European Commission Study on Trade Secrets, confirms that trade secret plays an important role in protecting the returns to innovation and that trade secret protection is an integral part of the overall system of protection in EU to protect intangible property. (EC Study, 2013) In this digital age, trade secret which is regarded as "gold nuggets" are facing threats from the risks associated with a global marketplace, rapid advances in technology and telecommunication, a mobile and highly skilled work force and networked strategic business relationship including outsourcing. (WIPO, 2002) The risks include theft of technical knowledge, procedural know-how, client data as well as attempts of corporate predators to acquire that information. (Heed, 2012). These threat actors thus can be in many forms such as malicious insiders, competitors, hacktivists and transnational organized crime. (CREATE, 2014) On this aspect, the US Treasury Department official has made a genuine statement reflecting the above situation that "Before, criminals used to steal money to become rich, but now they have realized that they can be rich by stealing corporate information." (Forbes, 2012)

Threats are becoming more eminent with the reliance on ICT to conduct and operate business. According to the US National Counterintelligence Executive, "cyberspace where most business activity and development of new ideas take place, allows malicious cyber-spies to quickly steal and transfer massive quantities of data while remaining anonymous and hard to detect. (Office of the Nat'l Counterintelligence, 2009-2011) The challenge, therefore, is to maintain the value of trade secrets. But maintaining the exclusive possession of valuable technical and commercial information in this competitive age equates fighting for financial survival. (Pace, 1995) This is due to the adverse impact of misappropriation that can cause tremendous loss to companies all over the world. (Holstein, 1998) According to a Report, the effects of intellectual property and trade secrets theft is twofold firstly tremendous loss of revenue and reward for those who made the inventions and secondly the theft undermines both the means and incentive for entrepreneurs of new inventions and industries that can further expand the world economy. (Report of the Commission on the Theft of American Intellectual Property, 2014)

The increased in the incident of theft of trade secrets could also due to globalization. According to the Report of the Commission on the Theft of American Intellectual Property, when large multinational companies expand their overseas operations, they almost inevitably face challenges related to supply accountability and protection against trade secrets. This is especially so when new piece of information that is sent overseas opens a company's supply chain and puts its valuable trade secrets at risks. (Report of the Commission on the Theft of American Intellectual Property, 2014) But the worst case scenario happened when the trade secrets become the target of cyber espionage. Often the time, a company did not realize that its sensitive information has been stolen and only discover the lost years later after huge financial losses has incurred. This type of espionage does not only become a domestic concern but also international trade community. (Skinner, 2014)

Due to economic and regulatory pressure and business expansion, most countries have resort to common law and/or civil law to deter theft of trade secret. But not many criminalize misappropriation of trade secrets. (EC Study, 2013) Question whether there should be criminal liability for the deliberate misuse of trade secret of another received mix global response. This is particularly so when misuse of trade secrets cannot be found a charge of theft due to the intangibility of the information. In the UK, this issue was debated and criticized in parliament

that “the theft of the board room table is punished for more severely than the theft of the board room secrets”. (Hansard, 1963) Despite various criticisms the criminal law in the UK is yet to protect trade secrets. The law maintains that trade secret cannot, in law, be stolen [since] they do not constitute “property” for the purpose of Theft Act 1968. Accordingly the court in the leading case of *Oxford v Moss* found an undergraduate student not guilty of stealing information which he memorized from a document because there is no intention to permanently deprive the owner of the document containing the information. Thus “if a trade secret is on a sheet of paper, a wrongdoer who removes it may be liable for theft of the paper, but a person who merely memories the secrets, and subsequently misuses it, incurs no criminal liability”. (UK LawCom, 2015) The Law Commission therefore found that the protection afforded to trade secrets by the existing law is limited.

Similar dilemma is faced by majority of commonwealth countries such as Malaysia and Australia. Malaysia, for example relies on common law to protect trade secrets but no protection afforded by criminal law. Thus when Malaysia signed the TPPA, Malaysia is obligated to criminalize theft of trade secrets and economic espionage. Thus this research propose to conduct bench marking exercise with the legal framework in the US, UK and Japanese legal system since they are signatories to the TPPA agreement. They are also among the five (5) countries that proposed for the criminalization of the theft of trade secret and Industrial espionage. The legal framework of these countries is briefly discussed below.

In the US, Civil protection is originally afforded by state law that protects trade secrets from improper acquisition, disclosure, and use of commercially valuable information that has been maintained in confidence. To maintain uniformity in application and enforcement of the law among the state, a creation of a civil cause of action for trade secret misappropriation under the federal law had been proposed resulting in the promulgation of the Uniform Trade Secret Act (UTSA). (Seaman, 2015) Mean while the common law protection is codified in Chapter 4 of the Restatement (Third) of Unfair Competition. It provides civil liability for improper acquisition of a trade secret if one has knowledge that it is a trade secret and also for unauthorized use of disclosure of a trade secret if one knows that (1) he acquired the trade secret under a duty of confidence; (2) he improperly acquired the trade secret; (3) he improperly acquired the trade secret from someone who acquired it improperly or breached a duty of confidence in disclosing

it; or (4) he acquired the trade secret through an accident or mistake unless this was due to the owner's failure to take reasonable precautions to maintain the secrecy of the information. The available remedy includes injunction, compensatory damages and an account of profit. (Yeh, 2014)

Some state laws also provide criminal liability for theft of trade secret. The statutes require proving of the act of theft which is intentional or that the trade secret was received or used with knowledge that it was stolen. But the criminal penalties vary according to states. At federal level, the Economic Espionage Act (EEA) 1996 protects "trade secrets of all business operating in the US, foreign and domestic alike, from economic espionage and trade secret theft. It also criminalizes espionage on behalf of a foreign entity and theft of trade secret for pecuniary gain. The definition of "misappropriation" under the Act imposes liability on any individual or entity that:

(1) steals, or without authorisation appropriates, takes, carries away, or conceals or by fraud, artifice or deception obtains a trade secrets;

(2) without authorization copies, duplicates, sketches, draws, photographs, download, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates or conveys a trade secret or

(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained or converted without authorization.

It also prohibits attempts and conspiracies to commit misappropriation.

Apart from the EEA1996, there are in existence several laws that criminalize misappropriation of trade secret for example trade secret misappropriation could be charged under the federal mail fraud and wire fraud. The law criminalizes the use of the federal mail and interstate wire or electronic communications to execute any scheme to deprive a person of his or her property or money. But the scopes of these laws are limited to mail, wire and electronic communications that excludes photocopy of the trade secret information and mere copy of the information because the victims is not permanently deprived of the data. (US CC, 2012)

The US government has relied on the National Stolen Property Act (NSPA) to prosecute the unauthorized transfer of trade secret information across state or foreign boundaries but this Act only applies if the defendant has knowledge that the trade secret has been stolen and then intentionally discloses it to a third party. However one limitation of this Act is that trade secret is not recognized as property thus prosecution is rather difficult unless there is proof of physical item storing the information.

Another federal Act that protects trade secret in the US is the Computer Fraud and Abuse Act (CFAA) 1986. The Act protects trade secrets that are computer-accessible. Originally enacted as a criminal anti hacking law for "information stored on computers belonging to the government and financial institutions, the scope has been broadened to firstly created civil remedy permitting "any person who suffers damage or loss" to pursue damages and injunctive relief", and secondly to include any computer "used in or affecting interstate or foreign commerce or communication" i.e. any computer capable of connecting to the internet. The Act created seven categories of prohibited conduct several of which can be invoked by trade secret plaintiff including:

1) Section 1030(a)(2) prohibits anyone from intentionally accessing any protected computer 'without authorisation or exceeding authorised access". The scope does not limit to trade secret only.

2) Section 1030(a)(4) prohibits the knowing access of a computer" without authorisation or that exceeds authorised access" with the "intent to defraud" and "by means of such conduct … obtaining anything of value".

The Act also provides civil liability that requires showing of addition harm to the plaintiff which can be satisfied by a damage or loss exceeding $5000 in value in one year period.

In addition, Tariff Act 1930 particularly section 337 can be invoked to combat extraterritorial acts of trade secrets misappropriation. The section confers authority to the US International Trade Commission ("ITC") an independent federal agency to conduct investigations of "unfair methods of competitions and unfair acts in the importation …or in the sale" of goods in the US. If violation is established, the ITC can issue an exclusion order preventing importation of the relevant good.

Therefore in the US, the government at both federal and state levels is rigorous in protecting trade secret. The growing and persistent threat by individuals, rival companies and foreign governments that seek to steal trade secrets has led to rigorous call for criminalizing the theft of trade secret despite the existence of trade secrets protection under both common law and by statute level. The US legal framework therefore consists of common law, civil and criminal actions through specific statutes as well as other relevant statutes. The US is also among the five members that proposed for the criminalization of the trade secret and economic espionage in the TPPA. (US CC, 2013)

United Kingdom and Malaysia are common law countries that rely on common law remedies for breach of trade secret and confidential information. The UK prior to the EU Trade Secret Directive does not have a codified civil statute to protect trade secrets but provides causes of action including trespass, conversion, conspiracy and interference with trade under the common law. As regards to criminal liability, the Fraud Act 2006 and the Computer Misuse Act 1990 imposes criminal liability for unauthorized taking, obtaining, or copying any document imposed criminal penalty up to ten years imprisonment. Thus UK legal framework therefore consists of the common law and criminal law under the general statutes. (OECD, 2015) UK Theft Act however is not applicable since trade secret and confidential information does not come within the definition of intangible property under the Act. (Oxford v Moss [1979] Cr. App. Rep 183)

In contrast to US, UK and Malaysia, Japan is a civil law country that provides civil and criminal liability under the Unfair Competition Prevention law. Article 2 of the law makes, inter alia, wrongful acquisition of a trade secret, using and disclosing the acquired trade secret and use them with knowledge as an act of unfair competition which entitles the owner for civil remedies such as injunction, destruction of the infringing articles and compensatory damages. Such wrongful acquisition is punishable under Article 21 of the law if the offender has the intent to acquire an illicit gain or to cause injury to the trade secret owner. The criminal penalty may extent to ten years imprisonment with labour, a fine of up to ten million yen or both. Cases where the defendant is found guilty will be widely publicised as deterrent purposes. (Kazuko 2012)

The above are three legal frameworks from countries that are members to the TPPA which could provide guidance for Malaysia to establish a legal framework to combat theft of trade secret and corporate espionage while at the same time protecting the value of trade secret.

Relevance to Goverment Policy

Malaysia has just signed the Trans-Pacific Partnership Agreement. The TPPA in Chapter 18 imposes criminal penalty on theft of trade secret and corporate espionage. Being a member Malaysia is bound by the terms of the agreement and must adhere to the requirement. The outcome of this research will serve as material source of reference for Malaysia to comply with the requirement.

Research Findings

A. There is no specific legislation available in Malaysia to address or deal with the protection of trade secret from theft or corporate espionage.

Being a common law country, we found that some protections for trade secret are available under the law of contract and confidential information. Employer would normally ask the employee to sign a confidentiality agreement to prevent the employee from disclosing any confidential information belonging to the employer during or after employment. Breach of the clause provides foundation for the employer to initiate civil action against the employee for breach of contract. This far we found no criminal action was taken against any employee who has use or steal trade secrets of the employer even though from the civil action there was evidence to show that the employee has stolen the information and sold or divulged the information to a rival for personal gain. This posed a serious risk and threat to the employer who has spent time and money to create the trade secrets. Two papers have been presented on this aspect at the International Conference on Law and Society (ICLAS 2018) in Kota Kinabalu Sabah in May 2018 entitled (i)"A Case Study on Misuse of Company's Confidential Information in Malaysia: Suggestion for Improvement" and (ii) "Protecting trade secret from theft and corporate espionage: Business Entity v Employee."

B. Whether Such Act Of Stealing Could Be Penalized

We then analyze the criminal law to see whether such act of stealing or theft could be penalized. But our finding is that theft only occurs if a tangible property has been stolen and since trade secret are intangible property such act cannot be criminalized. The reliance on tangible and physical property provides a hindrance for criminalizing such act of stealing a million dollar trade secrets. We also found that technology facilitates the act of theft online. The outcome of

this finding has also been presented at the ICLAS 2018 International Conference and the title of the paper is "Business under Threat: Under Which Law should trade secret theft be criminalized in Malaysia.

C. **Adequacy of the Communication and Multimedia Act 1998, the Computer Crimes Act 1997 and the Competition Law in comparison to Japan Unfair Competition Law and the US Economic Espionage Act**.

Most business kept their trade secret in the computer and hacking the computer may give access to the trade secrets. On this issue we found that the Communication and Multimedia Act 1998 and the Computer Crime Act 1997 are insufficient to penalize such crime. We have also analyze the Competition Law in Malaysia but the law can only be invoked if the use of trade secret is likely to bring about an anti-competitive effect. Thus a mere stealing or misappropriation of trade secret will not trigger the sanction of the Competition Act 2010.

Thus our analysis of the existing laws shows that there is no law that protects trade secret from theft or corporate espionage and the person who committed the act can easily escape punishment because there is no law to criminalize the act.

In contrast we found Japanese law provide both civil and criminal action to punish the act of theft and corporate espionage and the specific law that criminalize theft of trade secret and corporate espionage is the Unfair Competition Law which was introduced to combat the crimes in Japan and outside Japan. The US also criminalizes such act under the Economic Espionage Act 1990. Our research found that in 2006 the United States had commenced an action against a Chinese in the Northern District of California for economic espionage and the foreign entity identified was the Royal Malaysia Air Force together with Royal Thai Air Force and China's Navy Research Center. The alleged trade secret that was stolen was in relation to nVSensor belonging to a US company. In this case the criminal was sentenced to 24 months in prison. This case illustrates that Malaysia has been said to be involved with the crime of economic espionage by the criminal who was a Chinese citizen. In dealing with the issue of criminalizing theft of trade secrets and corporate espionage, we have presented a paper at the ASEAN LAW Institute Conference 2018 in Seoul entitled "Criminalizing Theft of trade Secrets and Corporate Espionage: Legal Issues and Challenges.

D. Trade secrets Protection and SME

In relation to trade secrets and SME, we found that SME and company in Malaysia are affected by theft of trade secret especially from their current and former employee. Case law shows that many employers have commenced civil action against their former employee for using their trade secret and/or disclose it to a rival company or to set up their own business similar to the former employee. From the cases that we have read, many employers have no knowledge on how to protect their trade secret and they did not clearly put the obligation on the current or former employee from disclosing their trade secrets. In contrast we found that major company like PETRONAS relied on contract and confidentiality provision in the contract to protect their valuable corporate information as well as by entering into a Non Disclosure Agreement when transacted with third party. On this point our finding is that SME and business entities in Malaysia has not use or rely on the law of trade secrets to protect their sensitive and valuable corporate data. This finding has been presented at ICLAS 2018 conference.

E. Online Theft and Cyber espionage

In relation to online theft of trade secrets and cyber espionage, we found that the Communication and Multimedia Act 1998 (CMA) and Computer Crimes Act 1997 (CCA) are in adequate to govern the crimes. The ransom ware attack has actually challenge the adequacy of these Acts to protect business industry from such attacked and intrusion. Our finding on these two laws are that the CMA and CCA has limitation in addressing these threat of ransom ware, online theft and cyber espionage and both laws requires amendment to fully address these threat. The outcome of this finding has been presented at the International Conference on IT for Cyber and IT Service Management, in Lake Toba, Medan, Indonesia on 7 August 2018.The paper won the Best Paper under the category of cyber security.

F. Threat To National Economy Is Not A National Crime In Malaysia

The Cyber Security Malaysia, the Royal Malaysia Police and several computer security companies confirmed that Malaysia is not free from this threat. The threats are not limited to hackers but also organized crimes and foreign state that are targeting the trade secrets and valuable corporate information. Such threat has potential to affect the business and commercial industry in Malaysia as well as the economy of the country. Looking at the US and Japan approach in addressing this issue, Malaysia has several choices whether to regard such threat as a

crime against the state thus criminalize such threat under national security law such as the Security Offence (Special Measures) Act 2012 (SOSMA), Prevention of Terrorism Act 2015 (POTA) and National Security Council Act 2016. However these laws focus only on terrorism and other acts of crime against the state. Commercial espionage is not regarded as crime against the states. The finding has been presented at the ICLAS 2018 conference.

G. If theft of trade secrets and corporate espionage is a crime, what would be a suitable punishment?

Our final research was on the suitable punishment for theft of trade secrets and cyber espionage. This is because trade secrets worth a high value thus what would be the suitable punishment for stealing such information. A research was conducted at the Centre for Commercial Law Studies, Queen Mary University, London. We found that the main legislation governing the crime is the UK Fraud Act 2006, Computer Misuse Act 1990 and Sentencing Guideline by the Crown Prosecution Office. The UK Theft Act 1968 was not applicable since trade secret and confidential information does not come within the definition of intangible property under the Act. The usual sentences for such crime are imprisonment and a fine. The period of imprisonment however varies from 2 years to 10 years with up to £5000 fine under the UK Computer Misuse Act 1990. The value of the loss or damage suffered resulting from the offence committed becomes the basis for determining the length of imprisonment and the fine under the Fraud Act 2006. However under the Computer Misuse Act 1990, the punishment and sentencing is solely based on the discretion of the court upon consideration of the charges, the nature of the crime, the background of the offender, the age and the extent of the damage done. The finding has been highlighted in the First IP & Innovation Researchers of Asia Conference, January 2019 at IIUM, Kuala Lumpur.

Recommendation

1. Protecting trade secrets from theft and corporate espionage is important because it ensure healthy growth of industry and boost the national economy especially with the 4.0 industrial revolution. The protection should be comprehensive in the sense that the law should protect the rights of the trade secrets owner from its employee and competitors against theft of trade secret and corporate espionage, should encourage healthy competition and those who steal the trade secret should be punished. Our law does

protect trade secrets under the common law of confidential information and contract law but we do not have law to punish those who steal the trade secrets for private gain or sell it to the competitors or to foreign agent. The US, the UK and Japan have civil laws protecting the trade secrets and criminalize theft of trade secrets and corporate espionage. It is important to note that a strong legal protection of trade secret will invite foreign investors to our country and this also would encourage technology transfer.

2. A strong legal framework is needed to ensure its protection. Since the threat of theft and corporate espionage can be in physical and online form, both criminal law and cyber law need to be strengthened to address and reduce the threat. The most important recommendation is to define trade secrets as a property in both tangible and intangible form as in the Japan Unfair Competition Law and the US Economic Espionage Act Once this is statutorily recognized, then stealing it in physical form will be an offence under the Penal Code. If it is in an intangible form, having access and copying it would amount to an offence under the Multimedia Communication Act 1998 and the Computer Crimes Act 1997.Civil remedies provides the owner of trade secrets a right to commence action against the employee and person under obligation and to seek relief and remedies such as injunction, damages and compensation, criminal sanction under the Penal Code and cyber laws will provide stronger legal framework to protect the commercial commodity value attached to the trade secrets. For the punishment and sentences of the crimes, the UK Fraud Act 2006 and the Computer Misuse Act 1990 provide useful guideline for consideration.

3. Malaysia should recognize a threat to national economy as a crime against the state. This is because terrorists and criminals are stealing trade secrets for commercial gain to fund their organization. The Security Offences (Special Measures) Act 2012 (SOSMA), Prevention of Terrorism Act 2015 (POTA) and National Security Council Act 2016 (NSCA) should be amended to give such recognition. The US through the Economic Espionage Act 1990 for example is aggressive in protecting their national economy by prosecuting any person including US citizen from stealing or conspiring to steal and sell

US company trade secrets to foreign country. The US regards such act as illegal transfer of economic wealth which would destroys the US national economy. In recent events, the stealing of trade secrets and economic espionage was the reason for the emergence of the trade war between the US and China.

4. Companies and SME must protect their trade secrets. The common law of confidential information and contract law should be relied upon as measures to protect their trade secrets. They should include both internal and technical measures to protect their trade secrets as part of the organization corporate governance strategy and to work with the relevant authorities when stealing of trade secrets occurred. Reporting of such crime should be made mandatory for such reporting will give the authorities such as the police, the MCMC and Cyber Security an opportunity to investigate the matter further and arrest the culprit. This will also serve as a warning to any person who intent or being coerce to conduct corporate espionage. Lesson should be learned from the ransom ware attack.

With this recommendation, the research has come to the end. We thank the Ministry of Higher Education for funding this research.

Publication

i. Juriah Abd Jalil, Addressing the Threats of Online Theft of trade Secrets and Cyber Espionage in Malaysia: The Legal Landscape. 6th International Conference on Cyber and IT Service Management (CITSM), Parapat, Indonesia 2018, Published online by IEEE XPlore (Scopus) on 28 March 2019.

ii. Juriah Abd Jalil, Halyani Hassan "Protecting Trade Secret from Theft and Corporate Espionage: Some Legal and Administrative Measures", Journal of Business & Society (IJBS) 2019 (awaiting publication)

iii. Juriah Abd Jalil*, Halyani Hassan, Nasarudin Abd Rahman, Raja Badrol Hisham Raja Mohd Ali, Duryana Mohamed, Ahmad Najib, "Business Under Threat: The Criminal Liability Of Trade Secret Theft In Malaysia" Journal of Business & Society (IJBS) 2019. (awaiting publication)

b) Additional Outputs

Detail list of other outputs e.g.: non-indexed journal, conference proceeding/ book/ book chapters/ policy paper etc.

i. Protecting trade secrets from theft and corporate espionage: Business entitied v employers, International Conference on Law and Society (ICLAS 7) 11-13th April 2018, Kota Kinabalu, Sabah.
ii. Business Under threat: Under which law should trade secret theft be criminalized in Malaysia, International Conference on Law and Society (ICLAS 7) 11-13th April 2018, Kota Kinabalu, Sabah.
iii. A case study on Misuse of Company's Confidential Information in Malaysia: Suggestion for Improvement. International Conference on Law and Society (ICLAS 7) 11-13th April 2018, Kota Kinabalu, Sabah.
iv. Criminalizing theft of trade secrets and corporate espionage: Legal Issues and Challenges (Malaysia, Japan & South Korea). ASLI Conference. 15th ASEAN Law Institute Conference, 10-11th May 2018.
v. Criminalizing theft of trade secrets and corporate espionage: Legal Issues and Challenges in Malaysia (Comparison with the development in the UK trade secret law), First IP & Innovation Researchers of Asia Conference, 31 January – 1st February 2019.
vi. Report On Data Collection At The Centre Of Commercial Law Studies, Queen Mary University, London conducted on the 26th – 31st November 2018. Submitted To RMC.

APPENDIX

REPORT ON DATA COLLECTION AT THE CENTRE OF COMMERCIAL LAW STUDIES, QUEEN MARY UNIVERSITY, LONDON FROM 26/11-31/11/ 2018

INTRODUCTION

The Centre of Commercial Law Studies (CCLS) has allowed us entrance and access to their postgraduate facilities and computer to enable us to find the relevant information for our data collection. The state of the art computer facilities and a conducive research environment has hastened our task and we were able to collect significant information relating to our research. The centre was kind enough to assign an officer to assist us and to arrange for interview with the experts at the Centre. The interview with Prof Ian Walden and Prof Maher Dabbah was scheduled on Tuesday, 27 of November 2018.

PART A: OUTCOME FROM THE INTERVIEW WITH PROF IAN WALDEN

The Interview was scheduled at 11am at the Centre. We received a warm welcome from Prof Walden who congratulates us on the research. Our focus of discussion was on the UK approach in dealing with theft of trade secret and economic espionage. The topic is divided into 3 namely:

1. Legislation in the UK that criminalize trade secrets theft and economic espionage;
2. Development of the UK law on trade secret protection in line with the EU Trade Secret Directive
3. Remedies and relevant penalty for theft and similar act.

In summary there is no legislation in the UK that criminalizes trade secret theft and economic espionage. The UK Theft Act is not applicable since trade secret and confidential information does not come within the definition of intangible property under the Act. Thus the UK is relying on Fraud Act 2006 and Computer Misuse Act 1990 to address the issue but both Acts only focus on the modus operandi or the commission of the crime rather than the subject matter of the

crime. In relation to the second topic, the UK has enacted the Trade Secrets (Enforcement, etc) Regulation 2018 to implement the EU Trade Secrets Directive 2016/943. However this legislation focuses on strengthening the civil remedies and common law protection of trade secrets. For remedies, the common law provides injunction, damages and account of profit for misappropriation of trade secrets and confidential information. Damages can be based on the value of the trade secrets and confidential information that is loss due to misappropriation of the same. In some cases payment of royalties or license fees are more appropriate. However these remedies are suitable for civil and common law action. For criminal punishment, analogy can be made with the punishment and sentences under the UK Theft Act 1968, UK Fraud Act 2006 and UK Computer Misuse Act 1990 and Sentencing Guideline by the Crown Prosecution Office. The usual sentences are imprisonment and a fine. The period of imprisonment however varies. Under UK Theft Act the punishment is imprisonment not more than 7 years. Punishment under UK Computer Misuse Act 1990 is from 2 years to 10 years with up to £5000 fine. Under the Theft Act 1968 and Fraud Act 2006, the value of the loss or damage suffered resulting from the offence committed becomes the basis for determining the length of imprisonment and the fine. This is provided under the Sentencing Guideline for theft and fraud. However there is no such guideline for offences committed under the Computer Misuse Act 1990, thus the punishment and sentencing is solely based on the discretion of the court. But the court will consider the charges, the nature of the crime, the charges, the background of the offender, the age and the extent of the damage done.

1. OUTCOME ON THE DISCUSSION ON UK LEGISLATIONS ON THEFT OF TRADE SECRETS AND ATTEMPT TO CRIMINALIZE MISUSE TRADE SECRETS

Our discussion began with the statistic that shows UK economy suffered loss of £ 9.2 billiondue to IP theft and £7.6 billionbecause of industrial espionage which make IP theft and industrial espionage range the top 2 crime in the UK.[1] We were informed that despite the large figure, the UK has no specific legislation to address this issue. Our further research on this matter found that

1 Detica Report. The Cost of Cybercrime. Cabinet office at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

the law of theft which is governed by the UK Theft Act 1968 focus on both tangible and intangible property however trade secrets and confidential information does not fall within this definition. This was due to the decision of the court in the case of *Oxford v Moss* [1979] Cr App Rep 183, an English criminal case law that dealt with theft of intangible property and information.

Section 1 of the Theft Act 1968 states, "A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it." There are three elements to constitute theft under this Act namely dishonestly, appropriation of property and intention to permanently deprive the other of it. In *Oxford v Moss* case a university student managed to obtain a proof copy of his forth coming exam paper and intended to return the document. He was charged with theft however cannot be convicted for theft because there was no intention to deprive the university of the property. He was then charged with stealing information belonging to the Senate of the University. At the magistrate court, the prosecution argued that the information itself was property capable of being stolen because it had attached to it a proprietary right of confidence and once this was breached, the information itself had been stolen. However the defence counsel argued that Sect 4 of the Act did not define a class of intangible property beyond a chose in action and therefore information per se was not protected by the Act. Accepting the defence argument, the magistrate rules that confidential information was not a form of property within the definition of sect 4 and that confidence consisted in the right to control the publication of the proof paper was merely a right over the property and not a property in itself. At the appellate level, the court dismissed the prosecution appeal and held that the definition of 'intangible property' was not broad enough to include confidential information and further held that in case involving confidentiality, the appropriate remedies for breach should be injunction or damages rather than criminal penalties. Similar decision was made in the case of *Absolom* (1979) 68 Cr App R 183. In this case a geologist obtained and attempted to sell to a rival company a record containing geological data and an indication of the prospects of finding oils that worth £50,000 to £100,000. Although the judge found that the geologist had acted in 'utmost bad faith', he was acquitted of theft on similar ground with *Oxford v Moss* case.

This decision is still applicable now making it difficult for the prosecution to charge and prosecute cases involving stealing or misappropriation of information.

In 1997, Lord Falconer of Thoroton QC, the solicitor general raised a concern in relation to the adequacy of the law to address the issue of commercial espionage. At the Denning lecture which was held in October 1997 prior to the Law Commission Consultation paper he said "one asks how is the law going to cope with the increasing prevalence of commercial espionage both by computer and otherwise where the commercial rival or predator obtains information which he then covertly uses to benefit himself in his dealings with the victim, for example by photocopying documents without authority, or by entering the victim's computer systems. No doubt the law will be able to concoct some niche in the criminal calendar. But it depends on the ingenuity of the prosecutor, the learning and advocacy of the defence, and the judge on the day. I welcome the fact that the Law Commission is due to publish a consultation paper next month looking at the operation of trade secrets."[Commercial Fraud or Sharp Practice – Challenge for the Law", Denning Lecture, 14 October 1997.]

Later in the same year, the Law Commission issued published a consultation paper highlighting the issue relating to criminalizing of trade secrets misused.[Law Commission for England & Wales, *Legislating the Criminal Code: Misue of Trade Secrets* (CP 150,1997) Consultation Paper on Misuse of Trade Secrets.] The consultation paper dealt with the issue of whether there should be criminal liability for the deliberate misuse of the trade secrets of another. The Commission acknowledged that the misuse of trade secrets cannot found a charge of theft. The paper deliberated on the inadequacy status of the criminal law and thus recommended a new criminal offence of misuse of trade secrets. The recommendation however was abandoned but due to the growing threatof theft of trade secrets and industrial espionage, perhaps the recommendation needs to be re-visited and considered.

In 1999, CD Freemen published an article on "The Extension of the Criminal Law to Protect Confidential Commercial Information: Comments on the Issues and the Cyber-Context" which he presented at the 14th BILETA Conference: "CYBERSPACE 1999: Crime, Criminal Justice and the Internet"(1999, Bileta). He agreed that the criminal law is an appropriate vehicle through which to deter the misappropriation of confidential commercial information and trade secrets, however cautioned must be taken to ensure the balance between the rationale for criminal liability and endangering other legitimate interest.

He highlighted that the commercial value of confidential commercial information has provides a primary justification for civil remedies and criminal sanctions to deter misappropriative activity in English law and elsewhere. This is because those trade secrets or "know-how" has always been an important asset. Therefore more protection is needed especially

when innovation become the central feature of post-industrial developed economies. On this aspect the threat to the security of the trade secret is apparent due to two reasons.First, the increase in the value of intellectual property and information arising from innovations in technology and secondthe rise in economic crime due to technological innovation and the internet.

Trade secrets and confidential information generates economic value particularly in investment. Being a secret allows an enterprise to be a head of others in a competitive environment. However, in the process of innovation, enterprise often has to share and exploit resources with other party in an attempt to create new product and wealth. In this sense the trade secret acted as both commodity (valuable in itself) and as a resources (to be exploited by commercial actors). The main challenge would be to share the secret information without the risk of destroying its value through illicit acquisition, use or disclosure by others such as a rival and by the third party.

Echoing the same point, Alberta Law Reform Institute further explain that technology makes today's business a race against time and that business advantage lies in technology. [Institute of Law Research and Reform and a federal Provincial Working Party, Trade Secrets (Report No.46, 1986) para 2.10-2.12) Consequently it creates intense business pressure to know what competitors are doing and one of the ways is by using technology to conduct espionage activity. In this sense, espionage becomes a real threat to business enterprise. This creates a business environment where information is critical within and outside the business where it is susceptible to misuse or unauthorized disclosure by those having control over it or being able to acquire it illicitly. It also affects the employee mobility. Because of this threat, Freemen was of the view that there is a need for effective deterrents against misappropriative act in order to maintain the value of informational assets and to protect the integrity of the innovation cycle. (1999, Bileta) However the nature of trade secrets that is intangible and indivisible makes it difficult to regulate. To tackle the problem, Freemen suggested the following steps before misappropriation of trade secret could be criminalized:

1. To properly analyze and evaluate the merits of criminalizing misappropriation of trade secrets by considering several questions namely what is the mischief to be remedied, what are the act that can be and should be criminalized and what public policy implication can arise from criminalizing such act;

2. To obtain proper evidence to ensure no trouble occurred after implementation of the criminal liability provision;
3. To understand the working of the misappropriative activity from two perspectve namely
    a. Private acquisition of the information through illicit means and without knowledge of the owner or person in possession of it, which is usually done by hackers or online theft;
    b. Disclosure by ex employee to new employers or to the relevant authority in the public interests.

In relation to the first, the main difficulty according to the Younger Commission is to draw the line between methods which consist of painstaking and legitimate gathering of business information and those which the law should treat as illegal. The problem stemmed from the lack of 'property' in trade secret and confidential information. It has legal implication in relation to criminal liability wherein the lack of property takes the misappropriative act outside the scope of the law of theft as seen earlier. This is similar to Malaysian law of theft under the Penal Code whereby the requirement of tangible property is primary and trade secret and information is not a tangible property. Further the term 'liability' is conditioned on the act itself being incidentally proscribed under the statute such as the UK Computer Misused Act 1990, the Copyright Designs and Patent Act 1988 and the Trade Mark Act 1988. On this point, Freemen agreed that the Law Commission has identified the significant gaps in extending criminal liability to misuse of confidential information and that criminal law ought to be able to relieve the decent and reputable trader's sense of helplessness in such circumstances.

In relation to the second criteria, disclosure by ex employee to new employers, the main issue in relation to criminal liability is whether criminal laws can be resorted to or fashioned where civil liability is itself insufficient. On this point the Law Commission recommended the creation of a new offence of misuse of trade secrets and it application is restricted to offensive conduct in relation to unauthorized use or disclosure of trade secrets. The rationale is to punish an offender who knowingly misappropriates valuable information that is not 'generally known'. The scope of the offence is not overly broad and actual prosecutions is to only instigated in the worst cases and where the availability of civil remedies is inadequate in the circumstances of individual cases. The sanction recommended is to punish employees, consultants or others who rightfully acquire information but then knowingly and intentionally misuse it. However the

model recommended does not include to illicit modes of acquisition or the question of industrial espionage.

Criminalizing misuse of confidential information also has implication on employee mobility. Many employees are skilled in technology and become technical experts and specialized managers who are active in the technology sectors. These experts often deal with valuable confidential information that is the primary assets of their employer and are often subject to confidentiality agreement. There is a huge demand for the expertise in the market place. But over protection of information through broad criminal liability may inhibit employee mobility and thus will indirectly slow the natural pace of innovation unjustifiably.

Consequently, English law remains passive in resorting to criminal law to address this issue of misuse of trade secrets. The UK law has made distinction between government, commercial and personal information within the equitable action of breach of confidence but such distinction has not be made in the incidental application of criminal law.The Law Commission has taken the position that criminal law in this area should be narrowly applied and ought to follow civil liability. In other words, criminal law should restrict itself to breach of confidence where the threat of civil liability in the circumstances is insufficient to promote compliance with express or implicit obligation of confidentiality. This approach is reflective of direct liability for unfair competition. The criminal law therefore should offer comprehensive protection for confidential commercial information by fulfilling three functions namely:

i. To set minimum standards of acceptable commercial behavior,
ii. To deter the breach of private obligation of confidence in appropriate circumstance as envisage by the Law Commission and
iii. To bring domestic treatment in line with emerging international standards respecting the protection of intellectual property through more liberalized unfair competition norms.

Cyber space provides a new avenue for Misappropriation of trade secret and economic espionage online. Thus what should be the standard of acceptable for regulating such behavior online. Freemen list out the following concerns:

(1) There is a need to set appropriate standards of commercial behavior in relation to confidential commercial information since misappropriation can be accomplished through the use of emerging technologies. On this aspect the function of the criminal law

in the commercial context is to define the outer limits of tolerable commercial behavior at the very minimum. Here criminal law plays a role that the civil remedies cannot. The difficulty would be in applying criminal sanctions where civil liability is uncertain. Nevertheless it is clear that one legitimate function for new criminal laws in this area is to set a threshold standard for commercial behavior under which criminal liability may be incurred.

(2) The criminal law should be able to provide general deterrence against wrongful acts where civil liability is inadequate. It is important to show that such wrongful acts liability and consequences. This is useful in enforcing commercial morality in the sense of deterring certain willful breaches of obligations of confidence in cyberspace or elsewhere.

(3) Criminalizing such act can deter money laundering and stop organized crime or terrorist from stealing and selling trade secrets a cross border. This could create a global response to such a trans-national problem. This is one of the mechanisms to stop economic espionage. On this point criminal law should aim to 'eradicate commercial practices' in relation to the misappropriation of valuable information where the nature of the conduct is sufficiently offensive. Such mechanism allows one to confront competitors who obtain trade secret illicitly through conventional methods and by technological means. This should be done in line with TRIPs, and Paris Conventions.

(4) Criminal law must be sufficiently precise to enable people to know whether they risk criminal liability for contemplated course of conduct and avoid inefficient enforcement of the criminal law through flawed prosecutions. Criminal liability may be established through complaint to the relevant authority and the while investigating, proper care need to be exercises since many victim are reluctant to make a complaint or engage in legal redress to avoid crises of investor confidence. Thus few complaints do not mean misappropriative activities does not occur.

(5) Need to be careful when relying of evidence or data by the industries because the focus would be more on the loss suffered or economic disaster rather than detailing types of conduct. The loss figures are based on expectation and not real loss.

Despite the above concern, the British government has not made any move to extend criminal protection to trade secret or making any attempt to criminalize misuse of trade secrets. However in mid December 2016, a case involving copying of a series of trade secrets by a disgruntled employee was heard at the Southwark Crown Court. (*CORBIERE LTD V KE XU*) In this case the an employee obtained accessed to his employer's computer system, copied a series of algorithmic trading codes with the attention to sell to a competitor and deleted a large number of records. He then fled to Hong Kong but was arrested and extradited back to the UK. Despite stealing his employer's trade secrets, he was charged with 'with fraud by abuse of his position' under Section 4 of the Fraud Act 2006. He was found guilty and sentenced to four years imprisonment. He was also charged for unauthorized access to a computer under the UK Computer Misuse Act 1990 however the action was not pursued against him. Rationale for charging under the Fraud Act 2006 rather than the Theft Act 1968 was because a thief could only steal the medium on which the secrets had been recorded or kept and that following *Oxford v Moss*, the trade secrets fall outside the meaning of property under the Theft Act. The fact that the value of the secret lies in the information itself and not the medium on which it was stored is not being considered by the court.

The employee was also charged under the Serious Crime Act 2007 and the court made an order known as "Serious Crime Prevention Order" ("SCPO"). Such order is usually used 'to protect the public, by preventing, restricting or disrupting a person's involvement in serious crime.' The order requires him to return physical copies of what he was alleged to have taken from his ex employer, the copies of the codes and his laptop. He failed to comply with some of the order and was sentenced to 18-month imprisonment. With such order made, 'stealing' trade secrets with intention to sell to rival and knowing that the trade secrets is valuable is considered as a serious crime in the UK, punishable by a period of imprisonment between 12 months to 5 years.Nevertheless the question remains what would be a suitable criminal penalty for those who maliciously remove the trade secrets of a business?

The Law Commission has highlighted the need to criminalize misuse of trade secrets as seen earlier but sadly the recommendation was not taken up. The UK prosecutor prefers to bring such cases under other act such as the Fraud Act 2006 and the Serious Crime Act 2007, rather than the existing Theft Act.The proposal for new crimes of misuse of trade secrets as recommended by the Law Commission in 1997 was also not taken up. The case nevertheless

invites comments especially on the charges brought against the employee. Farrer & Co for example said"The most interesting aspects of this case are the criminal offences for which Mr Xu was charged and one of which he was convicted. The fraud charge – fraud by abuse of position – is one which could well apply to many senior insiders who abuse the trust placed in them by their employers by copying materials (in this case, computer codes) for use by themselves or a new employer. Similarly, the use of a SCPO, in this case as pressure to return stolen material, is a potent weapon for the authorities." [Farrer & Co, Insight, January 2017 @ farrer.co.uk]

The other relevant legislation to govern misuse or misappropriation of trade secrets and confidential information is the Computer Misuse Act 1990. According to Prof Walden, the Act covers unauthorized access to computer to obtain the confidential information. Section 1 of the Act states:

(1) A person is guilty of an offence if— Unauthorised access to

(a) he causes a computer to perform any function with intent to computer secure access to any program or data held in any computer; material.

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.

This provision must be read together with section 17 and section 17 (2) state:

"A person secures access to any program or data held in a computer if by causing a computer to perform any function he—

(a) alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses it; or

(d) has it output from the computer in which it is held (whether by having it displayed or in any other manner);

and references to access to a program or data (and to an intent to secure such access) shall be read accordingly."

The Act focuses on an offence to secure access which makes a person who caused a computer to perform a function with intent to secure access, commits an offence. The provision however excludes mere physical contact with a computer and the scrutiny of data without any interaction with a computer such as reading of confidential information in the computer, reading of data displayed on the screen or computer eavesdropping. However the Act extended the offence to cover secondary liability to a person who supplies a hacker with information such as password and the operator of a computer hacker. The main *actusreus*for this offence is that the access to the program or data intends to secure must be 'unauthorized' access. As regard to *mens rea*, the two elements that must be proven are firstly there must be knowledge that the intended access was unauthorized and secondly there must have been an intention to secure access to any program or data held in a computer.

This provision applies to an employee who has authority to access certain client accounts but securing unauthorized access to document which she should not access. In the case of *R v Bow* [2002] 2 AC 216, the House of Lord held that an employee clearly came within the provisions of Section1 of the Computer Misuse Act 1990 when she intentionally caused a computer to give her access to data she knew she was not authorized to access. The House of Lord further held that an employee would only be guilty of an offence if the employer clearly defined the limits of the employee's authority to access a program or data.

As conclusion to the issue on criminalizing of theft of trade secrets, the UK law does not specifically criminalize the misappropriation of trade secrets. But several statutes namely the Fraud Act 2006, the Computer Misuse Act 1990 and the Serious Crime Offences 2007 have been use to criminalize the act of obtaining the trade secrets as seen above.

2. DEVELOPMENT OF THE UK LAW ON TRADE SECRET PROTECTION IN LINE WITH THE EU TRADE SECRET DIRECTIVE

The UK law of confidence that is based on common law and equity provides relatively strong protection against unlawful acquisition, use or disclosure. In June 2016, the EU Directive on the protection of undisclosed know-how and business information (trade secrets) against unlawful acquisition, use and disclosure ("the Directive") was introduced. The Directive aims to provide harmonizing legislation in relation to trade secrets protection in the EU that requires each national state to provide at least the same level of protection and minimum standards for measures, procedures and remedies. The directive requires its member state to implement the directive into its national law by 9 June 2018.

Responding to the directive, the UK Trade Secrets (Enforcement,etc) Regulations 2018 came into force after taking the following stand *"... where it is clear that measures are already provided for under current legislation, case law or courts rules, there is no need for [the UK] to implement these. Where there is uncertainty as to whether the provisions of the Directive apply across all legal jurisdictions, in order to put matters beyond doubt and ensure transparency, coherence and consistency, the Government has taken the view that certain provisions should be implemented fully."*

As a result a statutory protection of trade secrets was introduced into the UK law hand in hand with the common law of confidential information and equity law. The new UK law on trade secrets has therefore come into force.

Regulation 3, folds the Directive's definition of a trade secret into the UK's existing law of confidence in this manner:"*The acquisition, use or disclosure of a trade secret is unlawful where the acquisition, use or disclosure constitutes a breach of confidence in confidential information.*"

Regulation 2 of Act provides the definition of trade secret in line with the Directive which defines it as follow:

"trade secret" means information which –

(a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among, or readily accessible to, persons within the circles that normally deal with the kind of information in question,

(b) has commercial value because it is secret, and

(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret;"

Part (a) and (b) are the same with the current law in the UK however part (c) 'reasonable steps" introduces new element. The current UK law of confidence, it is necessary to show that the information was imparted in circumstances of confidence. (Coco v A.N Clark) But with the new requirement, business must show that they have taken steps to protect their information, otherwise they may lose such protection.

The new Regulation also introduces a provision on preservation of confidentiality of trade secrets in the course of proceedings under Regulation 10 which states as follows:

10.—(1) A participant, or a participant who has access to documents which form part of the proceedings, must not use or disclose any trade secret or alleged trade secret—

(a) which, on a duly reasoned application by an interested party or on a court's own initiative, a court by order identifies as confidential, and

(b) of which a participant has become aware as a result of participation in the proceedings or the access.

(2) The obligation referred to in paragraph (1) remains in force after the proceedings haveended, subject to paragraph (3).

(3) The obligation in paragraph (1) ceases to exist—

(a) where a court, by final decision, finds that the alleged trade secret does not meet therequirements of a trade secret, or

(b) where over time the information in question becomes generally known among, or readilyaccessible to, persons within the circles that normally deal with that kind of information.

(4) On a duly reasoned application by a party or on a court's own initiative, a court may orderany of the measures set out in paragraph (5) as may be necessary to preserve the confidentiality ofany trade secret or alleged trade secret used or referred to in the course of proceedings.

(5) A court may—

(a) restrict access to any document containing a trade secret or alleged trade secret submittedby the parties or third parties, in whole or in part, to a limited number of persons,

(b) restrict access to hearings, when trade secrets or alleged trade secrets may be disclosed,and to the record or transcript of those hearings to a limited number of persons, and

(c) make available to a person, who is not one of the limited number of persons referred to insub-paragraph (a) or (b), a non-confidential version of any judicial decision, in which thepassages containing trade secrets have been removed or redacted.

(6) The number of persons referred to in paragraph 5(a) or (b) must be no greater than necessaryto ensure compliance with the right of the parties to the legal proceedings to an effective remedyand to a fair trial, and must include, at least, one individual from each party and the lawyers orother representatives of those parties to the proceedings.

(7) In deciding whether or not to grant the measures in paragraph (5) in accordance withparagraphs (4) and (6) and which of the measures to order and in assessing the proportionality ofthe measures, a court must take into account—

(a) the need to ensure the right to an effective remedy and to a fair trial,

(b) the legitimate interests of the parties, and

(c) any potential harm for the parties.

(8) In this regulation—

"participant" means a party, a lawyer or other representative of a party, a court official, awitness, an expert or any other person participating in proceedings;

"parties", in paragraph (7), includes, where appropriate, third parties;

"proceedings" means legal proceedings relating to the unlawful acquisition, use or disclosureof a trade secret.

The holder of the trade secrets may apply for interim measure as provided under Regulation 11 however the court before making an order under regulation 11(1) may require the trade secret holder to provide evidence with a sufficient degree of certainty of the following under Regulation 12(1) that:

(a) a trade secret exists,

(b) the trade secret holder is making the application, and

(c) the alleged infringer—

(i) has acquired the trade secret unlawfully,

(ii) is unlawfully using or disclosing the trade secret, or

(iii) is about to unlawfully use or disclose the trade secret.

(2) In considering whether to make an order under regulation 11(1) and in assessing the proportionality of such an order, a court must take into account the specific circumstances of the case, including where appropriate—

(a) the value and other specific features of the trade secret,

(b) the measures taken to protect the trade secret,

(c) the conduct of the alleged infringer in acquiring, using or disclosing the trade secret,

Despite the enactment of the new regulation, UK law merely strengthened its protection for trade secrets in civil action since the Directive only provides the same. The Directive did not interfere with the national law of any member states that criminalize theft or misappropriation of trade secrets.

3. REMEDIES AND RELEVANT PENALTY FOR THEFT AND SIMILAR ACT

The law of confidence provides common law remedies such as injunction, damages and account of profit for misappropriation of trade secrets and confidential information. Damages can be based on the value of the trade secrets and confidential information that is loss due to misappropriation of the same. In some cases payment of royalties or license fees are more appropriate. However these remedies are suitable for civil and common law action.

Since there is no specific Act that criminalizes 'theft' of trade secret, punishment or sentences under the UK Theft Act 1968, UK Fraud Act 2006 and UK Computer Misuse Act 1990 can be used as comparison. Sentences under these statutes are imprisonment and a fine. The period of imprisonment however varies. Under UK Theft Act the punishment is imprisonment not more than 7 years. Punishment under UK Computer Misuse Act 1990 is from 2 years to 10 years with up to £5000 fine. The sentencing under the UK Fraud Act 2006 is guided by the Fraud Sentencing Guidelines. The guideline divided fraud offences into 5 types namely confidence fraud; possessing, making or supplying articles for use in fraud; banking, insurance and credit fraud; benefit fraud; and revenue fraud.

'Stealing' of trade secrets may falls under the confidence fraud that is a fraud where the perpetrator wins the confidence of the victim and obtains money or other property by deception. Such offences is usually charge under Section 1 of the Fraud Act and the sentence provides under this provision is 10 years imprisonment. Full sentence is usually reserved for serious criminal organization involving large scale frauds such as deliberate targeting of a number of victims. The number of years in prison will be determined by the value from the outcome of the fraud namely if the value is more than £500,000.00 the sentence is up to 7 years and where the value is between £200,000.00 and £100,000.00, the sentences would be up to four years.

The guideline also provides guideline to the judge to decide how serious the offence is and how blameworthy the defendant is when sentencing. In sentencing, the following will be considered:

1. The extent to which the offence was planned or opportunistic;
2. Whether the fraud is part of a 'professional' operation;
3. Whether it was carried out over a long or short period;
4. The willingness of the defendant and his or her motivation in carrying out the offence;
5. The value of the money or property involved;
6. Whether the offender was in a position of trust (for example an employee);
7. Whether a number of people were involved in the planning or carrying out of the offence;
8. The impact on the victim or victims, and how many there were;
9. Any risk of physical harm to another (e.g. burning down a building or staging an accident to obtain an insurance payment);
10. Whether less damage or loss was intended than actually ended up taking place;
11. Whether the defendant was in any way entitled to any of the property;
12. Whether there has been an attempt to conceal or dispose of evidence;
13. Whether the victim(s) were vulnerable and / or deliberately targeted;
14. Whether someone's identity has been used.

The guideline also highlighted that fraud is not a victimless crime and can cause considerable harm to society and the economy including closing down of business. As such apart from the above sentencing, the court may make ancillary orders such as compensation order (in cases where the victim has suffered financial loss or personal injury), confiscation order (where the defendant has benefitted financially from the offence and such order is in line with the Proceeds of Crime Act 2002), deprivation order (an order to deprive a convicted defendant of property used or intended to be used to commit an offence such as computer software and hardware),

restitution order (such as the stolen goods are restored to the victim or that the money equivalent to the value of the goods is paid to the victim form money seized from the defendants or assets owned by the defendant to that value are transferred to the victim), disqualification from acting as a company director (for offences relating to the running of a business and the ban could be 5 years in the Magistrate Court or 15 years in the Crown Court), financial reporting order (in cases where the court believe that the defendant are likely to be involved in the future in further offences of dishonesty) and lastly serious crime prevention order (to protect the public by restricting the convicted person's ability to be involved in serious crime as seen in the *Ke Xu* case).

Such official guideline for sentencing is absent for offence under the Computer Misuse Act 1990. In the case of *R v Mudd* [2018] 1 Cr App R(S) 33(7), a teenager who admitted of committing offences under section 1 and 3 of the Act for setting up a computer hacking business was only sentence to 21 monthsdetention at the young offender institution. Mudd has carried out and directed 1.7 million DDoS attacks over a million individual IP address or domain names. According to Michael Topolski QC the judge in this case his crime had wreaked havoc "from Greenland to New Zealand, from Russia to Chile".

Further, in relation to sentence based on the potential loss suffered from the fraud and unauthorized access, the Court of Appeal in the case of *R v Brown* [2014] EWCA 695 held that, that such potential loss is not the determining means by which fraud should be valued thus reduced the sentence from 3 years to two years imprisonment.Nevertheless in the case of *R v Martin* [2013] EWCA Crim. 1420 where the offender pleaded guilty to offences under Section 1,2,3 and 3A of the Computer crimes Act 1990, the Court of Appeal upheld his sentence of two years considering the prevalence of computer crime that compelled the organizations in this case, the Oxford and Cambridge University to spend substantial sums combating it. The court also stated that the potential impact on individuals meant that sentences for such offences should involve a real element of deterrence.

CONCLUSION

UK law does not specifically criminalize theft of trade secrets. However cases shown that person committed misappropriation of trade secrets has been under the Fraud Act 2006, Computer Misuse Act 1990 and the Serious Crime Prevention Order. On the other hand the UK law has

enhances the civil and common law protection of trade secrets by introducing the Trade Secret (Enforcement, etc) Regulation 2018 as required by the EU Trade Secret Directive. Such move has provides statutory definition of trade secrets and introduce new element to prove in a breach of confidence action. The regulation will harmonize trade secret protection throughout EU by providing the at least the same level of protection and minimum standards for measures, procedures and remedies. In term of criminal sanction, the Fraud Act, Computer Misuse Act impose imprisonment and fines and use the loss of value or damage suffered as a measure to determine the length of the terms of punishment. This provide a good input to Malaysia in terms of deciding what and how the punishment for theft of trades secrets and economic espionage.

Part B. COMPETITION LAW AND THEFT OF TRADE SECRET

Competition law seeks to protect the process of rivalry and provide a level playing field for enterprises to compete in the market. In other words, competition law promotes free competition in the market by eliminating anti-competitive conduct which may disrupt or distort the normal process of competition. Generally, competition law achieves its objectives through three important competition provisions, namely, prohibition against anti-competitive conduct, prohibition against monopolization or abuse of dominant position and prohibition against merger or anticipated merger that substantially lessens competition in the market.

a) Anti-competitive agreement

Competition law prohibits any form anti-competitive agreement between enterprises which has the object or effect of preventing competition, reduce uncertainties in the market and limit the ability of the enterprises to carry out their commercial decision independently. This covers both anti-competitive horizontal agreement such as price fixing, market sharing, bid rigging and sharing sensitive commercial information and anti–competitive vertical agreement such as exclusive dealing, resale price maintenance, tying and bundling etc.

The only relevant anti-competitive agreement in relation to theft of trade secret or industrial espionage is the sharing of sensitive commercial information between enterprises which may facilitate collusive behaviour in the market. However, it is

important to note that, before making decision on whether sharing information is anti-competitive and runs afoul the Competition Act 2010, the competition authority needs to prove the existence of agreement to share confidential information between enterprises. Agreement under the Competition Act 2010 is defined as "any form of contract, arrangement or understanding, whether or not legally enforceable, between enterprises…"[2]Theft of trade secrets or industrial espionage on the other hand involves an act of stealing commercial or corporate information which may undermine the competitiveness of an enterprise. Therefore, it is difficult to use anti-competitive agreement provision to combat theft of trade secrets due to the lack of element of consensus or meeting mind.

1. **INTERVIEW WITH PROF EYAD MAHER M.DABBAH, DIRECTOR OF INTERDISCIPLINARY CENTRE FOR COMPETITION LAW (ICC), QUEEN MARY UNIVERSITY OF LONDON**.

b) Abuse of dominant position

Section 10 of the Competition Act 2010 prohibits an enterprise holding a dominant position in the relevant market from abusing its dominant position. Abusive conduct under section 10 is very wide but in general it can be categorized into two: exploitative conduct and exclusionary conduct. Exploitative conduct refers to the ability of an enterprise to exploit the consumers such as by increasing prices above competitive level. Exclusionary conduct on the other hand refers to the ability of an enterprise to exclude an equally efficient enterprise.

The act of stealing of corporate information by large enterprise may be considered as an abusive and run afoul section 10 of the Competition Act 2010. For an example, a dominant big data company may steal confidential data from its smaller competitors or users in order to maintain or expand its market power. However, it is important to note that the application of competition law (under abuse of dominant position) is very much limited in scope depending whether or not an enterprise is holding a market power in the

2 Section 2, *Competition Act 2010*.

relevant market. The competition authority needs to determine the relevant market and dominant position before making conclusion that the act of stealing of trade secret by the said enterprise is abusive.

Competition law prohibits abuse of dominant position in any form. There were attempts to expand the scope of abuse of dominant position to the area of data or privacy protection. For example, in German, the competition authority is currently investigating Facebook for abuse of its dominant position in the social networking market on the basis that Facebook's terms of service violated data protection law, as they allowed Facebook unrestrictedly to collect user data from third-party sources). However, the conduct of Facebook is qualified as an exploitative as opposed to exclusionary conduct. It is still unclear at this stage whether competition law enforcement in the area of abuse of dominant position can or should be expanded to privacy or data-protection related activities. Even it is so, the scope of application is very limited and fails to capture the conduct of a non-dominant enterprise. The application of competition law in the area of date protection and trade secret requires strong and effective cooperation between regulators.

2. INTERVIEW WITH DR MARIA IOANNIDOU, DEP DIRECTOR OF INTERDISCIPLINARY CENTRE FOR COMPETITION LAW (ICC), QUEEN MARY UNIVERSITY OF LONDON.

c) Merger or anticipated merger that lessens competition in the market.

Merger control provision prohibits any merger that reduce the level of competition in the market. It focuses on the structure of the market rather than the behaviour of economic actors. An enterprise facing less competition in the market has the tendency to engage in an anti-competitive behaviour. Therefore, merger under competition law regime acts an ex-ante control of market concentration and monopolization.

Mergers and acquisition may be used by the acquiring enterprise to steal corporate information from the target enterprise. As a result, when the merger plan was aborted,

the acquiring enterprise will utilize all the stolen data to produce new products using competing technologies and know-how. Concerns about corporate espionage by foreign acquiring enterprise has become a source of concerns particularly when it involves sensitive technologies and operations. Due to this emerging threat, many competition authorities around the world are now starting to recognize national security as one of important considerations in merger assessment. The competition authority may block any merger which poses a threat to national security such as the transfer of sensitive technology or know-how outside a country, foreign surveillance and espionage, threat to social and economic stability etc.

PART C UNFAIR COMPETITION LAW AND THEFT OF TRADE SECRET

Unfair competition law promotes both free and fair competition in the market while competition law promotes effective and free competition. Unfair competition law mainly protects the competitors' interest while the main function of competition law is to protect the process of competition. The main objective of unfair competition law to prevent dishonest and unfair commercial practices which cannot be resolved through competition law. For example, unfair competition law prohibits abuse of economic dependence by business that do not hold a dominant position in any relevant market.[3]

Corporate espionage may be seen as a form of unfair competition in the market as it involves misappropriation of information which is proprietary and valuable. [4]An enterprise may obtain corporate information or trade secret belong toits rivals through various illegal means putting the thieves in a competitive advantage vis-à-vis the victim enterprise. With the advance of technology, the modus operandi of corporate espionage become more sophisticated and complex. Many countries around the word including German, China, Korea and Japan had formulated unfair competition law to combat corporate espionage and theft of trade secret. However, unfair competition law is not all about preventing corporate espionage but rather a general law that

3 European Parliament, Briefing Paper on Addressing Unfair Practices in Business-to- Business Relations in the Internal Market (2011) p 15

4Tucker, Robert L, "Industrial Espionage as Unfair Competition" (1998). Akron Law Publication. 213

promote fair trade and commercial practices. Below are the objectives of four unfair competition law:

Section 1 the Act against Unfair Competition (German) "protecting competitors, consumers and other market participants against unfair commercial practices. At the same time, it shall protect the interests of the public in undistorted competition".

Article 1, Law of the People's Republic of China Against Unfair Competition, "to safeguarding the healthy development of socialist market economy, encouraging and protecting fair competition, repressing unfair competition acts, and protecting the lawful rights and interests of business operators and consumers." (China)

Article 1,Unfair Competition Prevention and Trade Secret Protection Act (Korea)–"to maintain orderly trade by preventing acts of unfair competition such as improper use of domestically well-known trademarks and trade names, and by preventing infringement of trade secrets".

Article 1, Unfair Competition Prevention Act (Japan) – "to provide measures, etc. for the prevention of Unfair Competition and for the compensation of damages caused by Unfair Competition, in order to ensure fair competition among business operators".

Four unfair competition law regime under study incorporated provisions against obtaining and disclosing trade secret without the consent of owner of the trade secret. For example, under unfair competition laws, unfair competition practices include:

KOREA

"Using or disclosing trade secrets to obtain improper benefits or to damage the owner of the trade secrets while under a contractual or other duty to maintain secrecy of the trade secrets"(Korea)

JAPAN

"the act of using or disclosing a Trade Secret that has been disclosed by the business operator that owns said Trade Secret (hereinafter referred to as the "Owner") for the purpose of acquiring a wrongful gain, or causing damage to said Owner" (Japan)

CHINA

(1)obtaining an obligee's trade secrets by stealing, luring, intimidation or any other unfair means;

(2)(disclosing, using or allowing another person to use the trade secrets obtained from the obligee by the means mentioned in the preceding paragraph

GERMAN

(1)Whoever as the employee of a business communicates, without authorisation, a trade or industrial secret with which he was entrusted, or to which he had access, during the course of the employment relationship to another person for the purposes of competition, for personal gain, for the benefit of a third party, or with the intent of causing damage to the owner of the business shall be liable to imprisonment not exceeding three years or to a fine.

(2)Whoever for the purposes of competition, for personal gain, for the benefit of a third party, or with the intent of causing damage to the owner of the business, acquires or secures, without authorisation.

Trade secret is defined as follows:

KOREA

“information, including a production method, sale method, useful technical or business information for business activity, that is not known publicly, is the subject of considerable effort to maintain its secrecy and has independent economic value”.

CHINA

“any technology information or business operation information which is unknown to the public, can bring about economic benefits to the obligee, has practical utility and about which the obligee has adopted secret-keeping measures”

JAPAN

"technical or business information useful for business activities, such as manufacturing or marketing methods, that is kept secret and that is not publicly known."

SCOPE OF UNFAIR COMPETITION LAW

The scope of unfair competition law is still unclear and differs from one jurisdiction to another. China for example, combines both competition and unfair competition law in its Unfair Competition Act. This may create tension as competition law is not concerned about the well-being of competitors. Unfair competition law regime has its origin in intellectual property law such as trademarks and trade secrets and consumer protection law such as misleading conduct and false advertisement. In view of many consumer protection and IPRs legislations had been put in place, it is unclear what should unfair competition law covers. It is also important to ensure whether additional protection of IPRs and consumer through unfair competition legislation is necessary. Since unfair competition law has its origin IPRs and consumer protection, unfair competition law always provides for civil remedies rather than criminal sanctions. However, the German unfair competition law contains both civil remedies and criminal sanctions. Under German Unfair Competition Act disclosure of trade and industrial secrets carries imprisonment not exceeding three years or to a fine.[5]

CONCLUSION

Competition law is still inadequate to prevent theft of trade secret and industrial espionage due to some requirements that need to be fulfilled under anti-competitive agreement and abuse of dominant position provision. Merger control provision allows the competition authority to block merger that could lead to industrial espionage but the prevention is only limited to mergers and acquisition exercise. Unfair competition law can be used to resolve the inadequacy of competition law in resolving the issue of industrial espionage. However, the scope of unfair competition law should be clear so as to avoid overlapping with existing legislations relating to consumer protection and intellectual property. Malaysia may follow German's footstep in criminalizing theft of trade secret by having two-remedial action regime.

5 Section 17, Act Against Unfair Competition (2010)

PREPARED BY:

ASSOC. PROF. DR. JURIAH ABD JALIL AND DR NASARUDIN ABD RAHMAN