Worldwide Challenges Impairing Enforcement of Trade Secret Protection

by Noor Asyikeen bt Mohd Salleh*

Noor Asyikeen bt Mohd Salleh; Advocate and Solicitor of the High Court of Malaya, LL.B (Hons) IIUM, Associate at Messrs Iza Ng Yeoh & Kit, Selangor.

Abstract

The purpose of this paper is to examine a number of challenges impairing enforcement of trade secrets protection globally wherein further research and development are encouraged to be performed towards providing effective protection of trade secrets comprehensively. The first challenge is that current laws protecting trade secrets and efforts to enforce them in many countries remain relatively weak. Secondly, the worldwide growing numbers of cyber economic espionage and theft of trade secret. Last but not least, employment mobility affecting trade secret protection.

Introduction

World Intellectual Property Organization ("WIPO") defined trade secrets as any confidential business information which provides an enterprise a competitive edge such as customer lists, methods of production, marketing strategies, pricing information, and chemical formulae.[1] Well-known examples of trade secrets include the formula for Coca-Cola, the recipe for Kentucky Fried Chicken, and the algorithm used by Google's search engine.[2]

At international level, protection of trade secrets is provided by the World Trade Organization's 1994 TRIPS Agreement (Agreement on Trade-Related Aspects of Intellectual Property Rights). Article 39.2 of the TRIPS Agreement specifically provides that trade secrets are protected as undisclosed information and such protection must apply to information that is secret, that has commercial value and that has been subject to reasonable steps to keep it secret.[3]

It is no doubt that trade secrets are increasingly valuable in today's businesses. A study in 2010 was conducted by Forrester Consulting who surveyed on Australian, European and the United States ("US") companies, regarding their data security practices.[4] Based on the study report, it shows that trade secrets amounted to 80% of the value of a company's information.[5]

In 2008, the National Science Foundation conducted a survey on the importance of various forms of intellectual property ("IP") protection to US companies businesses.[6] As summarised in the table below, it shows that trade secrets protection is the most important form of IP protection.[7]

* Advocate and Solicitor of the High Court of Malaya, LL.B (Hons) IIUM, Associate at Messrs Iza Ng Yeoh & Kit, Selangor

1 WIPO, "What is a Trade Secret?" *available* at http://www.wipo.int/sme/en/ip_business/trade_secrets/trade_secrets.htm.

2 Brian T. Yeh, "Protection of Trade Secrets: Overview of Current Law & Legislation", (2014) p.summary.

3 WIPO, "Overview: The TRIPS Agreement", *available* at https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm.

4 U.S. Chamber of Commerce, "The Case for Enhanced Protection of Trade Secrets in the Trans-Pacific Partnership Agreement," p.10.

5 *Ibid*. p.10.

6 *Ibid*. p.10.

7 *Ibid*. p.10.

Table 1.
Importance of Various Forms of IP Protection to US Businesses

	Very	Somewhat	Not
Trade Secrets	45%	22%	33%
Trademarks	33%	27%	40%
Utility Patents	26%	15%	60%
Copyrights	25%	25%	49%
Design Patents	15%	18%	67%

Although the value of trade secrets continues to increase, studies show that today's businesses face snowballing threats to their valuable trade secrets assets. It is reported that theft of trade secrets and other critical business information costs businesses billions of dollars in annual losses.[8] A recent study by PricewaterhouseCoopers ("PwC") and the Center for Responsible Enterprise and Trade ("CREATe.org") suggested that the economic loss attributable to trade secrets theft is between 1% to 3% of US Gross Domestic Product.[9]

The impact of trade secrets theft and espionage are felt by companies of every income level and in every region. It is expected that trade secrets theft and the losses caused by such theft to be on the rise.[10] This is because of the use of cyberspace, advanced computer technologies, and mobile communication devices, making the theft relatively anonymous and difficult to detect.[11]

Thus, a robust protection and effective enforcement of trade secrets are critical to a company's ability to innovate and grow in the market. Be that as it may, there are a number of challenges impairing enforcements of a trade secret. One of the challenges is that current laws protecting trade secrets and efforts to enforce them in many countries remain relatively weak.[12] Another great challenge to the enforcement of trade secret is due to the growing numbers of cyber economic espionage and theft of trade secret. Last but not least, employment mobility is also a challenge to the protection of trade secret. Each of these challenges shall be discussed in great details.

Laws in Protecting Trade Secrets and Efforts to Enforce Them in Many Countries Remain Relatively Weak

At present, trade secret protection is far from uniform across countries because it is primarily domestic in nature. Meaning that it is a matter of law to the respective country only. Many jurisdictions such as Australia, Brunei, Canada, Malaysia, New Zealand and Singapore provide protection for trade secret based on common law and equity alone.[13] Each of these jurisdictions, the contours of the law and the available causes of action are different.[14]

Furthermore, such countries do not have specific laws criminalising trade secret disclosure or misappropriation. Many of those countries only have criminal laws targeting computer-related crimes but do not address trade secrets directly.[15] Apart from that, the punishments often vary among those countries that provide criminal penalties on trade secret misappropriation. The comparative table below is a summary of penalties by which states punish trade secret infringer from a criminal standpoint.[16]

Table 2.
Various Penalties of Trade Secret Misappropriation in Different Countries

Country	Penalties
Japan	Imprisonment with work up to 10 years AND/OR monetary fine up to JPY 10,000 000.
Estonia	Imprisonment up to one year OR monetary fine.
Poland	Imprisonment from one month to two years OR monetary fine.
Romania	Imprisonment from six months up to two years OR monetary fine.
US	Imprisonment from six months up to 10 years OR monetary fine.

8 *Ibid*. p.10.
9 Brian T. Yeh, "Protection of Trade Secrets: Overview of Current Law & Legislation", (2014) p.18.
10 *Supra*. p.3.
11 *Supra*. p.summary.
12 U.S. Chamber of Commerce, "The Case for Enhanced Protection of Trade Secrets in the Trans-Pacific Partnership Agreement," p.3.
13 For Australian jurisdiction *see* Kathy Bowrey, Michael Handler, Dianne Nicol "Australian Intellectual Property: Commentary, Law and Practice", Oxford University Press (2010) p.526. For Malaysian jurisdiction see Tay Peck San "Intellectual Property Law in Malaysia: Confidential Information", Sweet & Maxwell Asia (2013) p.675.
14 *Ibid*. p.23.
15 *See* Malaysia's Computer Crimes Act (1997), *available* at http://www.agc.gov.my/Akta/Vol.%2012/Act%20563.pdf; Singapore's Computer Misuse and Cybersecurity Act (2007), *available* at http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId:8a3534de-991c-4e0e-88c5-4ffa712e72af%20%20Status:inforce%20Depth:0;rec=0.
16 European Commission "Study on Trade Secrets and Confidential Business Information in the Internal Market" (2013) p.66.

Weaker rule of law and lack of criminal penalties among countries, contribute to fostering vulnerabilities and access points for theft of trade secrets. Furthermore, trade secret owners have limited legal recourse when their rights are violated particularly when it involves parties from different countries and jurisdictions.[17] This is because many countries around the world do not have a uniformed standard of legal protection for trade secret that is applicable to other jurisdictions.

In the US, trade secrets are afforded by statutory protection such as the US Uniform Trade Secrets 1985 ("UTSA") and the Economic Espionage Act 1996 ("EEA"). However, in India, the trade secret protection is not yet expressly recognised as an intellectual property right.[18] Thus, Indian Courts have relied on equitable and common law (contractual obligation, Indian Contracts Act 1872) remedies as a means of protecting trade secrets.[19]

Delhi High Court in *John Richard Brady & Ors v Chemical Process Equipments P. Ltd & Anor* AIR 1987 Delhi 372, the Court held that there was an implied confidentiality and that the defendant was liable for the breach of the confidentiality obligations. In *Mr Anil Gupta & Anor v Mr Kunal Dasgupta & Ors* 97 (2002) DLT 257, the court granted an injunction against the defendants as there was a confidential obligation between the parties.

The Indian cases above show that the Indian Courts do recognise trade secrets protection but India is still lacking a single uniform statutory legal protection for trade secret which is applicable in other jurisdictions, unlike the US. This is one of the challenges concerning trade secret protection and enforcement. It may jeopardise a US customer's IP rights over a trade secret in India unless he or she carefully employs certain contractual mechanisms that are enforceable in India.[20]

In 2002, an ex-employee of an Indian software vendor, Geometric Software Solutions Ltd., was attempting to sell proprietary software source code owned by SolidWorks, a US client of the person's ex-employer, to the US client's competitors.[21] The ex-employee was caught red-handed in a sting operation, but he could not be effectively prosecuted in India because the source code was considered a trade secret and Indian law did not recognise "misappropriation" of trade secrets[22]. Furthermore, the US client did not have any contractual arrangements with the ex-employee in which it could directly enforce its rights against the ex-employee.[23]

Similarly, in 2004, an employee at an India-based software development centre of a US customer, Jolly Technologies, misappropriated portions of the company's source code by purportedly uploading and shipping files that contained source code for a key product to her personal Yahoo e-mail account.[24] Although the theft was detected in time to prevent the employee from distributing the stolen code, the US customer also could not successfully prosecute the employee because of the same gap in Indian IP law.[25]

These cases indicate that legal protection divergences and a lack of procedural mechanisms among countries often make intolerable enforcement actions for cross-border trade secret infringements, which are remarkably expensive and troublesome.[26] The abovementioned scenarios have drawn close scrutiny and served as a wake-up call to the Indian government as well as to the global community to strengthen international IP regime. This is also important in promoting to the foreign investor community that each country takes foreign IP seriously.

Cyber Espionage and Theft of Trade Secret

The great development of innovation in cyberspace and advanced computer technologies has brought many benefits to the world. Be that as it may, modern technology also enables global access and transmission instantaneously which has made it easier for thieves to steal valuable business information. For the last few decades the world had moved into a whole new realm of spying: cyber espionage.[27] Cyber espionage is among the utmost challenges of protecting trade secret because tracing the sources of cyber espionage is notoriously difficult, given the facts of ubiquity and anonymity of the Internet.[28]

17 *Supra.* p. summary.
18 Abhinav Kumar, Pramit Mohanty & Rashmi Nandakumar, "Legal Protection of Trade Secrets: Towards a Codified Regime" Journal of Intellectual Property Rights, Vol. 11, November (2006) p.398.
19 Law Library of Congress, "Protection of Trade Secrets: India", *available* at http://www.loc.gov/law/help/tradesecrets/india.php. p.1.
20 Sonia Baldia, "Offshoring to India: Are your trade secrets and confidential information adequately protected?" available at https://www.mayerbrown.com/files/Publication/c4321838-f2ec-4fe5-990d-1ea497a7398b/Presentation/PublicationAttachment/5a87579c-8d2b-469d-ad3d-bb95435fe6ff/ART_OFFSHORINGTOINDIA_0308.PDF. p.10.
21 *Ibid.* p.10.
22 *Ibid.* p.10.
23 *Ibid.* p.10.
24 *Ibid.* p.11.
25 *Ibid.* p.11.
26 U.S. Chamber of Commerce, "The Case for Enhanced Protection of Trade Secrets in the Trans-Pacific Partnership Agreement," p.24.
27 Dana Rubenstein "Nation State Cyber Espionage and its Impacts", available at http://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/. p.1.
28 James Pooley "Trade Secrets the other IP right", *available* at http://www.wipo.int/wipo_magazine/en/2013/03/article_0001.html. p.3.

The rise of cyber theft affects the economic and political relationships between nation-states as well as changing the shape of modern warfare.[29] According to a recent study by security firm McAfee, "every company in every conceivable industry with significant size and valuable intellectual property and trade secrets has been compromised (or will be shortly)."[30] Thus, cyber espionage is a cross-border problem which needs to be addressed by governments around the world.

Generally, cyber espionage refers to an act of targeting secret information for malicious purposes.[31] Tallinn Manual (a guideline for nation-state cyber warfare concluded in a conference hosted by the NATO Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia) which was published in 2013 defines cyber espionage as "an act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party."[32] The definition of cyber espionage given by the Tallinn Manual is essentially important because it allows victim nations to take appropriate countermeasures against foreign cyber attacks for even the slightest intrusion.[33]

Digital technology influences cyber espionage in a number of unexpected ways.[34] Malware such as viruses, worms and Trojan horses are among popular tools for disrupting normal computer operations by secretly collecting data or destroying it entirely.[35] Another kind of attacks includes "Logic Bombs" using a process known as "spear-phishing".[36] It is a malware which is designed to lie dormant in another computer system. Once the embedded link is clicked, the thief's malicious software invades the recipient's computer and network.[37] This silent invader searches for important confidential files and passwords and sends all the information back to the hacker who uses or sells the information.[38]

The abovementioned attacks are examples of common kinds of computer attacks which can be devastating if carried out on a large scale.[39] At the international level, cyber espionage is becoming more advanced, effective and professional. Economic espionage and trade secret theft by foreign entities are often carried out by powerful large entities with specific government sponsorship and backing.[40] A report by the US Office of the National Counterintelligence Executive has estimated losses from such economic espionage to be in the tens or even hundreds of billions of dollars annually to the American economy.[41] It is indeed huge losses to a country.

It appears that the nation-states cyber espionage does not only engage in the realm of warfare but is also employed as cyber tools against each other to steal economic and financial data as well.[42] The US, Russia and China are among major players in the cyber espionage game.[43] It is reported that China is more interested in using confidential information for the purpose of building its own economy, rather than for political advantage.[44] According to an intelligence report, the China's People Liberation Army ("PLA") is not only capable of advanced surveillance and espionage, but also possesses malware that can take down foreign electricity or water grid.[45]

Recently, the nation-state cyber activity which receives the most public attention is espionage between the US and China. For many years the US has accused China of attempting to steal confidential information from the US.[46] In the last few years, it is reported that Chinese hackers have attempted cyber attacks on 2,000 companies, universities and government agencies in the US.[47] Recently, trade secret theft has hit some of US's best-known companies such as DuPont and Goodyear.[48]

---

29 *Supra.* p.1.
30 Pamela Passman "Trade Secret Theft: Businesses Need to Beware and Prepare", *available* at http://www.forbes.com/sites/ciocentral/2012/05/24/trade-secret-theft-businesses-need-to-beware-and-prepare/. p.2.
31 *Supra.* p.2.
32 *Ibid.* p.2.
33 *Ibid.* p.2.
34 *Ibid.* p.4.
35 *Ibid.* p.4.
36 James Pooley "Trade Secrets the other IP right", *available* at http://www.wipo.int/wipo_magazine/en/2013/03/article_0001.html. p.3.
37 *Ibid.* p.3.
38 *Ibid.* p.3.
39 Dana Rubenstein "Nation State Cyber Espionage and its Impacts", *available* at http://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/. p.4.
40 Randall C. Coleman "Testimony on Combating Economic Espionage and Trade Secret Theft", *available* at https://www.fbi.gov/news/testimony/combating-economic-espionage-and-trade-secret-theft. p.1.
41 *Ibid.* p.1.
42 Dana Rubenstein "Nation State Cyber Espionage and its Impacts", *available* at http://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/. p.5.
43 *Ibid.* p.2.
44 *Ibid.* p.5.
45 *Ibid.* p.2.
46 *Ibid.* p.5.
47 *Ibid.* p.5.
48 Randall C. Coleman "Testimony on Combating Economic Espionage and Trade Secret Theft", *available* at https://www.fbi.gov/news/testimony/combating-economic-espionage-and-trade-secret-theft. p.1.

In the case of DuPont (*United States v Liew*), two men were charged with stealing DuPont's secret recipe for making titanium dioxide and selling it to a Chinese competitor.[49] The recipe is used to whiten the cream inside Oreo cookies which can also be used for the manufacture of paper and plastic product as well.[50] The process involves chloride, which is highly regarded as a cleaner.[51] It is considered as a more efficient process than using sulfates in the normal standard manufacturing process.[52] DuPont controls a significant portion of the global market for titanium dioxide, and thus has taken great measures in keeping this formula as a trade secret.[53]

The court found that Robert Maegerle, an engineer who had been working with DuPont for 35 years, had disclosed the recipe to Walter Liew who had set up a California company with the intention of producing the titanium dioxide and selling it to Pangang Group, a Chinese competitor.[54] Walter Liew had entered into contracts with Chinese state-owned entities for the projects involving the use of the titanium dioxide technology for manufacturing purposes.[55] Evidence showed that after obtaining the trade secret, the parties sold it for over USD20 million.[56] On 5 Mar, 2014, in a San Francisco federal court, a jury convicted Walter Liew and Robert Maegerle for economic espionage and theft of trade secrets developed by DuPont.[57]

Another case involving economic espionage is *United States v. Chung* 659 F.3d 815 (9th Cir. 2011). In this case, Chung, a former engineer for the US-contractor Boeing, was found in possession of over 300,000 Boeing documents, including six documents containing Boeing trade secret.[58] Chung's lawyers argued that there was insufficient evidence as to the existence of any Boeing trade secrets within the documents that he possessed.[59] The court examined the Boeing documents relating to a NASA space-shuttle antenna thoroughly.[60]

Judge Graber found that Boeing maintained the secrecy of its information and enacted reasonable protective measures to maintain its secrecy.[61] The court reasoned that such information could assist a competitor in understanding how Boeing approaches problem-solving and in figuring out how best to bid on a similar project in the future, for example, by underbidding Boeing on tasks at which Boeing appears least efficient.[62] Thus, the court held that Boeing's secret information was independently valuable not for Boeing's potential use, but for the use of such information by any potential Boeing competitor.[63]

The US is not the only nation under attack from economic espionage and theft of trade secret. In fact, economic espionage and theft of trade secret occur all around the world. In 2013, a survey was conducted on companies in European countries: about 20% of the respondents reported having experienced at least one attempt or act of misappropriation over the past 10 years, while about 40% stated that risk has increased during that period.[64]

In 2007, Japan's Ministry of Economy, Trade, and Industry surveyed 625 manufacturing firms and revealed that more than 35% had suffered from some technology loss.[65] The Canadian Government discovered in 2010 that the same scenarios also happened to almost 86% of Canada's large corporations, and that the rate of cyber espionage in the private sector had doubled since 2008.[66] This trend appears consistent across economies.[67] South Korea reported in 2008 that its firms had lost USD82 billion due to foreign economic espionage; that number is up from USD26 billion in 2004.[68] Likewise, the United Kingdom estimates that theft of trade secrets accounts for over 40% of the USD34 billion annual cost of industrial espionage to its private sector.[69]

Indeed, from the above statistics, it is clear that cyber espionage has had significant impacts not only to the companies, but also to the nation as a whole. The result of

49 2014.
50 Brooklyn Law School "Trade Secrets Institute: Cases from Economic Espionage Act", *available* at http://tsi.brooklaw.edu/category/legal-basis-trade-secret-claims/economic-espionage-act. p.3.
51 *Ibid*. p.3.
52 *Ibid*. p.4.
53 *Ibid*. p.4.
54 *Ibid*. p.4.
55 *Ibid*. p.4.
56 *Ibid*. p.4.
57 *Ibid*. p.3.
58 *Ibid*. p.3.
59 *Ibid*. p.3.
60 *Ibid*. p.3.
61 *Ibid*. p.3.
62 *Ibid*. p.3.
63 *Ibid*. p.3.
64 Jennifer Brant & Sebastian Lohse "Trade Secrets: Tools for Innovation and Collaboration 2014", International Chamber of Commerce (ICC) 2014, p. 14.
65 U.S. Chamber of Commerce, "The Case for Enhanced Protection of Trade Secrets in the Trans-Pacific Partnership Agreement," p.12.
66 *Ibid*. p.12.
67 *Ibid*. p.12.
68 *Ibid*. p.12.
69 *Ibid*. p.12.

economic espionage and theft of trade secret is not only the initial monetary loss, but also the risk of losing money and jobs in the future.[70] Furthermore, the consequences of nation-state cyber espionage can be harmful to the future of international relations and national security.[71]

In a nutshell, cyber espionage and theft of trade secret are one of the most important and intriguing international problems in the world today. Trade secret protections will always be a challenge. Therefore, this alarming threat should be taken seriously by all countries. Every country and corporate sector should come up with appropriate safeguards and countermeasures against such peril.

One effective way of overcoming the challenge is by regulating the development of international law to allow cross-border prosecution and enforcement of trade secret. It is also important to regulate strong criminal sanctions that can both complement and fill gaps in existing civil remedies.[72] Apart from that, it is also essential to enhance domestic law operation on protecting trade secret by improving the domestic legislation. Last but not least, raising public awareness on the importance of protecting trade secret should be part of the strategy call for every nation.

Employment Mobility

The global trend of greater job mobility is affecting trade secret protection as it naturally increases the risk that employees will use their former employer's trade secrets in subsequent employment.[73] Greater mobility in career paths can reduce employment security and subsequently may weaken loyalty between employees and companies.[74] Furthermore, greater job mobility increases the risk of creating more opportunities for employees to use a previous employer's trade secrets in subsequent employment — whether accidentally or intentionally.[75] As employee mobility continues to rise, companies will face greater challenges in protecting their trade secrets.[76]

A study in 2008 showed that some 60% of those accused of misappropriating confidential business information in the US were current or former employees[77] and statistics from the Economic Espionage Act ("EEA") database also indicate that 76% of the defendants in EEA cases were current or previous employees of the company bringing claims of misappropriation.[78] It is a prevalent global trend as can be seen as well in India, being the number one destination for outsourcing services involving information technology and business processes[79]. Surveys reveal that a majority of cases of data misconduct arise from employees or ex-employees of a service provider.[80]

In fact, many developing countries in Asia have very high employee turnover rates.[81] In Malaysia, the annual employee turnover rate has in past years reached over 12%.[82] Rapid growth is fueling the rise in employee mobility and though such growth is highly desirable from an economic point of view, strong measures are needed to counter the rise in trade secret misappropriation due to that mobility.[83]

Threats of trade secret misappropriation from current or former employees can be overcome by careful contractual mechanism and the common law tort of "breach of confidence" irrespective of the existence of a contract would also be applicable.[84] However, overzealous use of non-compete clauses can cause it to backfire to the company. In the cases of *D'Sa v. Playhut, Inc.*[85] and *Latona v. Aetna U.S. Healthcare, Inc.*[86] whereby the US Courts of California agreed that the non-compete provisions of their new employment agreements were void against public policy and that they could not be legally terminated for declining a void contract.[87]

---

70 Dana Rubenstein "Nation State Cyber Espionage and its Impacts", *available* at http://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/. p.8.
71 *Ibid.* p.8.
72 U.S. Chamber of Commerce, "The Case for Enhanced Protection of Trade Secrets in the Trans-Pacific Partnership Agreement," p.18.
73 *Ibid*, p. 13.
74 Charles Cronin & Claire Guillemin, "Trade Secrets: European Union Challenge in a Global Economy", *International Fragrance Association*, p. 4
75 U.S. Chamber of Commerce, "The Case for Enhanced Protection of Trade Secrets in the Trans-Pacific Partnership Agreement," p.13.
76 *Ibid.*
77 Jennifer Brant & Sebastian Lohse "Trade Secrets: Tools for Innovation and Collaboration 2014", International Chamber of Commerce (ICC) 2014, p. 16
78 *Supra.*
79 Sonia Baldia, "Offshoring to India: Are your trade secrets and confidential information adequately protected?" *available* at https://www.mayerbrown.com/files/Publication/c4321838-f2ec-4fe5-990d-1ea497a7398b/Presentation/PublicationAttachment/5a87579c-8d2b-469d-ad3d-bb95435fe6ff/ART_OFFSHORINGTOINDIA_0308.PDF. p.9.
80 *Ibid*, p. 10.
81 U.S. Chamber of Commerce, "The Case for Enhanced Protection of Trade Secrets in the Trans-Pacific Partnership Agreement," p.13.
82 *Ibid.*
83 *Ibid.*
84 Sonia Baldia, "Offshoring to India: Are your trade secrets and confidential information adequately protected?" *available* at https://www.mayerbrown.com/files/Publication/c4321838-f2ec-4fe5-990d-1ea497a7398b/Presentation/PublicationAttachment/5a87579c-8d2b-469d-ad3d-bb95435fe6ff/ART_OFFSHORINGTOINDIA_0308.PDF. p.10.
85 Cal. App. Lexis 982 (2000).
86 82 F. Supp. 2d 1089 (C.D. Cal. 1999).
87 Faulkner, "Trade Secret Litigation: New Challenges When Using the Employment Contract to Protect Trade Secrets, Confidential Information, and Competitive Advantage" *available* at www.finnegan.com.

Under the Common Law, such clauses may fall under the prohibition against restricting one's right to earn a living. Hence, the challenge is to protect the company's trade secrets whilst at the same time not to unjustly deprive the employee his right to earn a living based on his knowledge and know-how. In the US, under the EEA, a person should not be prevented from using general business knowledge to compete with a former employer[88] as it is believed that employees who change their employers or start their own company should be able to apply their talents without fear of prosecution. It is not enough to say a person has accumulated experience and knowledge during the course of his or her employment and that the individual is inappropriately using such knowledge.[89]

Apart from the above, the current law in Malaysia provides only civil remedies. Though trade secret theft could possibly, to a certain extent, be prosecuted under criminal offences such as criminal breach of trust, no such case has yet been undertaken. Because of this, many companies chose to forgo civil suits because the thief is essentially judgement proof. Even if a company does bring suit, the civil penalties often are absorbed by the offender as a cost of doing business and the stolen information retained for continued use.[90]

The followings are examples of cases involving trade secret misappropriation by former employees:

United States[91]:

In 2012, South Korea-based Kolon Industries, Inc. and several of its executives were charged for allegedly conspiring to steal trade secrets from American firm DuPont and Japanese firm Teijin. DuPont's Kevlar and Teijin's Twaron para-aramid fiber had been widely known as commercially available para-aramid fiber products for decades. Para-aramid fiber is used to make body armor, fiberoptic cables, and automotive and industrial products. Kolon wanted to develop a para-aramid fiber to compete with Kevlar and Twaron. Between July 2002 and February 2009, Kolon hired current and former employees of the two firms to serve as "consultants" and asked them to reveal proprietary information, including details of the manufacturing process, customer and price lists, costs and profit margins, market trends, and business strategies. DuPont had sued Kolon in a related civil case in 2009. However, immediately after DuPont filed its summon, key Kolon employees deleted a substantial number of emails in violation of the law. Despite this loss of evidence, DuPont was able to prove its case against Kolon, winning a USD920 million verdict and an injunction. However, this verdict is being appealed, and in the meantime, Kolon has been permitted to continue selling its para-aramid products.

Japan:[92]

In 2012, Japanese-based Nippon Steel Corporation sued South Korean steelmaker Posco in both the United States and Japan for alleged theft of trade secrets related to electrical steel sheet technology. This technology is used in power plants' electric generators, hybrid cars, and vibration motors in mobile phones. Nippon Steel alleges that the theft has cost it as much as USD1.23 billion. The information was allegedly passed to Posco by a former Nippon Steel employee. This case is still pending.

Malaysia:[93]

In 2012, Malaysian plastics company Plastech Industrial Systems sued former employees and a competitor company for unlawfully taking and using its proprietary information and breaching the duty of confidentiality. Evidence showed that the former employees had held high management positions at Plastech and thus had full access to Plastech's technical specifications, pricing lists, costs, customer information, and status of on-going negotiations. While still employed at Plastech, they formed a company to compete with Plastech and used Plastech's trade secrets to gain customers and suppliers for this new company. Unlike Plastech, which invested in extensive research to develop its products, the new competing company engaged in no research and development and was only able to produce plastic products identical or similar to Plastech's products by using Plastech's trade secrets. The High Court ordered an injunction, return of all proprietary information and products produced using proprietary information, and an assessment of damages.

The above scenarios reveal that job mobility increases the risk that employees will use their former employer's trade secrets in subsequent employment. It is another challenge in protecting the trade secret of the company, given the facts of mobility of the employees. Therefore, corporate sector should come up with appropriate safeguards and countermeasures against such threat. Furthermore, a combination of robust civil enforcement as well as criminal penalties is important for protection of trade secrets.[94]

---

88 Chris Carr & Larry Gorman, "The Revictimization of Companies by the Stock Market Who Report Trade Secret Theft Under the Economic Espionage Act", *The Business Lawyer, Volume 57, Number 1, November 2001, pages 25 – 53*, p. 35.
89 *Ibid*, p. 36.
90 *Ibid*, p. 33.
91 U.S. Chamber of Commerce, "The Case for Enhanced Protection of Trade Secrets in the Trans-Pacific Partnership Agreement," p.20.
92 *Ibid*, p. 21.
93 *Ibid*, p. 22.
94 *Ibid*.

Conclusion

In conclusion, there are many challenges to protecting trade secret, inter alia, no uniform laws and the enforcement in many countries remain relatively weak, the snowballing numbers of cyber economic espionage and theft of trade secret as well as employment mobility. Unlike in the US and Sweden, there is no statutory protection provided for trade secrets in many countries around the world, and victims must resort to improvised measures such as contractual mechanism and whatever remedy is available under the Common Law.

For example within the European Union, trade secrets law is still perceived mostly as a matter of unfair competition rather than of IP.[95] Hence, unlike other forms of intellectual properties, trade secrets protection is not expressly recognised as an IP right in many countries. Therefore, there is a wake-up call to recognise trade secrets under a centralised uniformed statutory protection throughout countries. Otherwise, cross-border prosecution, enforcement and remedies of trade secret misappropriations will seem impossible.

The need for a more effective protection of trade secrets is made more pressing in light of the globalised competition and nation-backed as well as private-driven corporate and cyber espionage. Without appropriate measures and safeguards, companies will continue to exploit information value with or without them realising it and in the growing competitive global market, such disadvantage could be catastrophic.

A development of International Law for effective cross-border enforcement is also necessary. In light of the continued 'warfare' approach of the major powers of the US, China and Russia, this may be as good as impossibly hoping for world peace. Despite that, strong domestic protection through a uniformed and comprehensive legislative work should first be made before pressing for any international reforms between competing nation-states and foreign entities.

References

1. Abhinav Kumar, Pramit Mohanty & Rashmi Nandakumar, "Legal Protection of Trade Secrets: Towards a Codified Regime" Journal of Intellectual Property Rights, Vol. 11, November (2006)
2. Brian T. Yeh, "Protection of Trade Secrets: Overview of Current Law & Legislation", (2014)
3. Brooklyn Law School "Trade Secrets Institute: Cases from Economic Espionage Act", available at http://tsi.brooklaw.edu/category/legal-basis-trade-secret-claims/economic-espionage-act
4. Cal. App. Lexis 982 (2000)
5. Charles Cronin & Claire Guillemin, "Trade Secrets: European Union Challenge in a Global Economy", *International Fragrance Association*
6. Chris Carr & Larry Gorman, "The Revictimization of Companies by the Stock Market Who Report Trade Secret Theft Under the Economic Espionage Act", *The Business Lawyer, Volume 57, Number 1, November* (2001)
7. Dana Rubenstein "Nation State Cyber Espionage and its Impacts", *available* at http://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/
8. European Commission "Study on Trade Secrets and Confidential Business Information in the Internal Market" (2013)
9. Faulkner, "Trade Secret Litigation: New Challenges When Using the Employment Contract to Protect Trade Secrets, Confidential Information, and Competitive Advantage" *available* at www.finnegan.com
10. James Pooley "Trade Secrets the other IP right", *available* at http://www.wipo.int/wipo_magazine/en/2013/03/article_0001.html
11. Jennifer Brant & Sebastian Lohse "Trade Secrets: Tools for Innovation and Collaboration 2014", International Chamber of Commerce (ICC) (2014)
12. Kathy Bowrey, Michael Handler, Dianne Nicol "Australian Intellectual Property: Commentary, Law and Practice", Oxford University Press (2010)
13. Law Library of Congress, "Protection of Trade Secrets: India", *available* at http://www.loc.gov/law/help/tradesecrets/india.php
14. Malaysia's Computer Crimes Act (1997), *available* at http://www.agc.gov.my/Akta/Vol.%2012/Act%20563.pdf
15. Pamela Passman "Trade Secret Theft: Businesses Need to Beware and Prepare", *available* at http://www.forbes.com/sites/ciocentral/2012/05/24/trade-secret-theft-businesses-need-to-beware-and-prepare/
16. Randall C. Coleman "Testimony on Combating Economic Espionage and Trade Secret Theft", *available* at https://www.fbi.gov/news/testimony/combating-economic-espionage-and-trade-secret-theft
17. Singapore's Computer Misuse and Cybersecurity Act (2007), *available* at http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId:8a3534de-991c-4e0e-88c5-4ffa712e72af%20%20Status:inforce%20Depth:0;rec=0
18. Sonia Baldia, "Offshoring to India: Are your trade secrets and confidential information adequately protected?" *available* at https://www.mayerbrown.com/files/Publication/c4321838-f2ec-4fe5-990d-1ea497a7398b/Presentation/PublicationAttachment/5a87579c-8d2b-469d-ad3d-bb95435fe6ff/ART_OFFSHORINGTOINDIA_0308.PDF
19. Tay Peck San "Intellectual Property Law in Malaysia: Confidential Information", Sweet & Maxwell Asia (2013)
20. U.S. Chamber of Commerce, "The Case for Enhanced Protection of Trade Secrets in the Trans-Pacific Partnership Agreement,"
21. WIPO, "Overview: The TRIPS Agreement", *available* at https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm
22. WIPO, "What is a Trade Secret?" *available* at http://www.wipo.int/sme/en/ip_business/trade_secrets/trade_secrets.htm
23. 82 F. Supp. 2d 1089 (C.D. Cal. 1999)

[95] Charles Cronin & Claire Guillemin, "Trade Secrets: European Union Challenge in a Global Economy", *International Fragrance Association*, p. 3