Achieving Strategic Advantages through Protecting Trade Secrets

陳靖塘*1
朝陽科技大學台灣產業策略發展博士學位學程兼任助理教授

摘要
The concepts of intangible assets, intellectual property, and intellectual capital will first be introduced, and how a company may achieve a strategic advantage by dynamically transforming intangible assets into intellectual property (IP, such as trade secrets, patents, copyrights, trademarks) and further into intellectual capital will be explained, whereas the critical role played by trade secrets in this transformation will be highlighted. Then, the legal regime of trade secrets protection in Taiwan will be introduced and compared with the Uniform Trade Secrets Act (UTSA) and The Economic Espionage Act of 1996 (EEA) in the United States. Finally, strategies for protecting trade secrets for multinational companies in Taiwan will be suggested, whereas protections provided by civil law, criminal law, corporate procedures, and information security policies will be particularly addressed. By adapting these protections, a company may achieve a more efficient allocation of intellectual property resources, thereby achieving a sustainable strategic advantage.

關鍵字：trade secret, intellectual property, intangible asset, economic espionage

*陳靖塘 E-mail：freedomofoperation@gmail.com Tel：0975571783
1. INTRODUCTION

A company may gain competitive advantage by effectively converting its intangible assets into intellectual capital. A company possesses various intelligence in regard to the market, competitors, customers, suppliers, and products. When the intelligence is organized in a meaningful way, it becomes a company's intangible assets. For example, when a company creates a customer mailing list, it has transformed its intelligence in regard to its customers into an intangible asset. Today, it is estimated that over half of a company’s value may be attributed to its intangible assets.

A company's intangible assets play a crucial role in creating, or sometimes even destroying, the company's competitive advantage, which can be achieved through transforming intangible assets into intellectual capital. Although intellectual capital has been the subjects of many studies, most notably by Stewart, there is yet a generally accepted definition of intellectual capital. In this paper, we will define intellectual capital as "packaged intangible assets." When an intangible asset is packaged, it can then be exploited, leveraged and shared.

There are many ways to package intangible assets. One primary way is to convert these intangible assets into intellectual property, thereby allowing them to be protected under the intellectual property law. Intellectual property generally includes patents, trade secrets, copyrights and trademarks, but can also include service marks, trade dress, trade names, domain names and semiconductor chip designs.

Usually, it is clear which of these intellectual properties a company should choose to protect its intangible assets. For example, if a company wants to protect its original works of authorship fixed in a tangible medium, then it should seek protection under the copyright law. However, tension frequently exists between patents and trade secrets. When the subject to be protected is a
patentable invention, a company must choose whether to patent the invention or to keep it as a trade secret.2

To patent the invention, the patentee may enjoy the right to exclude others from making, using, selling, or distributing the invention.3 The legal right offered by the patent law is typically stronger than trade secrets right, which not only varies from jurisdiction to jurisdiction, but also can be difficult to enforce. On the other hand, patenting an invention requires making the invention available to the public and the protection offered is limited in time.4 Trade secrets right, to the contrary, can continue indefinitely, but the right is lost once the secret is made public or reverse engineered. Therefore, strategic IP planning requires balancing the invention's patentability, the estimated product lifecycle, the possibilities of reverse engineering, and the technology transfer business model.

2. Trade Secrets Law in Taiwan, China, and the United States

As previously mentioned, the trade secrets law varies from jurisdiction to jurisdiction. This paper will now present the legal regime of trade secrets protection in Taiwan, China, and the United States.

2.1 Trade Secrets Law in Taiwan

In Taiwan, trade secrets law covers any method, technique, process, formula, program, design, or other information that may be used in the course of production, sales, or operations.5 To qualified as a trade secret, the information must not be known to persons generally involved in the information of this type, and must have economic value due to its secretive nature.6 In addition, the owner must have taken reasonable measures to maintain the information’s secrecy.7

In Taiwan, once a secret owner has reason to believe that the secret has been improperly acquired by a competitor, the secret owner usually has many options, both civil and criminal. On the civil side, the secret owner may seek
infringement damages under the Trade Secret Act, tort damages under Article 184 of the Civil Code, and contract damages under the employment agreement. On the criminal side, the infringer faces criminal prosecution for fraud under Article 342 of the Criminal Code, for failure to preserve commercial secrets under Article 317 of the Criminal Code, and for computer crime under Article 318-1 of the Criminal Code.

2.2 Trade Secrets Law in China

In China, similarly, the Anti-Unfair Competition Law covers trade secrets on technical information and business information. To qualified as a trade secret, the information must be utilized to create business interests or profit for its legal owners, and must be unknown by the public. In addition, the legal owners must maintain the information's secrecy. In addition to the Anti-Unfair Competition Law, a trade secret may also be protected by Contract Law under Article 43 of the Contract Law, by Company Law under Articles 149-150 of the Company Law, by Labor Law under Articles 22 and 102 of the Labor Law, and by Labor Contract Law under Article 23 of the Labor Contract Law.

As previously discussed, both China and Taiwan offer comprehensive legal protection for trade secrets. However, even with the protection in place, China and Taiwan are usually not the ideal jurisdiction for seeking trade secret misappropriation damages. Due to the fact that the legal systems in China and Taiwan are civil law systems, a plaintiff there usually must carry a higher initial burden of proof in convincing the court that a trade secret has been misappropriated. To carry out this burden, the plaintiff must be ready to produce evidences without the help of the civil discovery mechanisms, which remain very limited in these countries. Moreover, in both countries, a police raid action and an ex-parte civil filing for “preservation of evidence” are rarely granted. Therefore, the ideal jurisdiction for trade secret litigation is often in the United States.
2.3 Trade Secrets Law in the United States

In the United States, a trade secret is protected by the state trade secret law, Section 337 of the Tariff Act, and the Economic Espionage Act of 1996.

2.3.1 Uniform Trade Secrets Act

Although trade secrets law is determined by state law, most states now have adopted the Uniform Trade Secrets Act (U.T.S.A.) published by the Uniform Law Commission. Under the U.T.S.A., a trade secret includes “formula, pattern, compilation, program, device, method, technique, or process” that “derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and … is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.”

A trade secret is misappropriated if the trade secret is acquired by a person who “knows or has reason to know that the trade secret was acquired by improper means.” A trade secret is also misappropriated if the trade secret is disclosed or used by another without express or implied consent by a person who used improper means to acquire knowledge of the trade secret.

In practice, most trade secret litigations focus on whether a secret owner has used “reasonable efforts” to maintain the trade secret’s secrecy and whether a defendant has acquired the trade secret through “improper means.”

To show that “reasonable efforts” have been used to maintain the secrecy, the court does not require the owner to take extreme and unduly expensive procedures, but only efforts that are “reasonable under the circumstances.” Therefore, this is largely a fact-intensive issue, and usually not readily subject to resolution on summary judgment. For example, the Fifth Circuit holds that it would have been unreasonable to ask the secret owner to cover his unfinished factory with a temporary roof during construction just to protect others from taking
photos of the factory from the sky. When trying to convince the court that “reasonable efforts” have been taken, the secret owner must keep in mind of the rationales behind the “reasonable efforts” requirement, which include (1) failure to take reasonable efforts is persuasive evidence that the secret has no value, (2) courts won’t spend resources to assist a secret owner who fails to take minimum steps to protect his secret, and (3) failure to take reasonable efforts sets a trap to competitors, who have no reason to believe that the information is a trade secret.

Even if the secret owner takes reasonable efforts to maintain the secrecy, to prove misappropriation, the secret owner still must show that the defendant took the secret by “improper means.” According to the U.T.S.A., improper means includes “otherwise lawful conduct which is improper under the circumstances.” Although the list of the improper means is not possible, U.T.S.A. does offer some examples of the proper means, which includes discovery by independent invention, discovery by reverse engineering, discovery under a proper license, observation in public, and obtaining the trade secret from published literature. Generally, this issue requires a close factual analysis and is rarely proper to be disposed by a summary judgment. In most cases, to constitute "improper means," there must be some classified wrongful conduct involved, such as breach of a confidential relationship.

Once the secret owner can show that the trade secret is misappropriated by the defendant using improper means, the secret holder may be entitled to both injunctive relief and damages. Under the U.T.S.A., a court may order an injunctive relief when actual or threatened misappropriation had happened. The duration of the injunction usually lasts until the trade secret has ceased to exist, but may also continue for a reasonable period of time to compensate for the change of position. In addition, the U.T.S.A. authorizes the court to compel the misappropriator to conduct affirmative acts to protect a trade secret. For example, the court may order the misappropriator to return the fruit of the stolen trade secret. In rare occasions, such as when overriding public interest exists,
the court may order the misappropriator to pay reasonable royalty during the prohibited period in lieu of issuing an injunction.29

Except for cases where a material and prejudicial change of position would render a monetary damages inequitable, the court may award the secret owner monetary damages, which include both the actual loss suffered by the secret owner and the unjust enrichment of the misappropriator.30 As an alternative, the court may also award the secret owner reasonable royalty for the misappropriator’s unauthorized disclosure or use of the trade secret.31 Moreover, when the defendant misappropriates the trade secret willfully and maliciously, the court may award the secret owner up to twice the amount that otherwise would have awarded.32 In addition, when the misappropriation is conducted in bad faith, or willfully and maliciously, the court may award the secret owner attorney’s fees.33

2.3.2 Economic Espionage Act

The Economic Espionage Act of 1996 makes economic espionage and the misappropriation of a trade secret federal crimes. The Act has been used to target foreign companies since its enactment, most notably in the Four Pillars Enterprise Company case and the Yuen Foong Paper Manufacturing Company case, both Taiwanese companies.34 Although the courts in both cases did not impose severe criminal penalty to the individual defendants involved, enormous resources were spent by the two companies for the prosecutions.35

Under 18 U.S.C. § 1831, "[w]hoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly ... steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret ... shall ... be fined not more than $500,000 or imprisoned not more than 15 years, or both.”36 Under 18 U.S.C. §1832, “[w]hoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof,
and intending or knowing that the offense will injure any owner of that trade secret, knowingly steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information shall ... be fined under this title or imprisoned not more than 10 years, or both."

Under the Act, a "trade secret" includes all forms and types of "financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing" as long as the secret owner has taken reasonable measures to keep its secrecy and the information derives "independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public ...."38

2.3.3 Section 337 of the Tariff Act

Although Section 337 of the Tariff Act (Section 337) is frequently used by domestic companies to prevent the importation of products that infringe U.S. patents, the scope of the Section 337 investigation is not so limited. In fact, Section 337 permits the International Trade Commission (ITC) to prevent importation of products based on trade secret misappropriation that occurred outside the United States.39

Under Section 337, the ITC may investigate "[u]nfair methods of competition and unfair acts in the importation of articles . . . into the United States" when the unfair acts cause injury to a domestic industry.40 In TianRui, the Federal Circuit affirms that the ITC may grant relief based in part on trade secret misappropriation happened entirely outside the United States, if it is necessary to protect domestic industries from unfair competition in the domestic marketplace.41
In reaching the choice of law issue, the Federal Circuit holds that “a single federal standard, rather than the law of a particular state, should determine what constitutes a misappropriation of trade secrets sufficient to establish an [‘]unfair method of competition[’] under section 337.”

Although what the “federal standard” for the trade secrets law remains an open question, for the Chinese legal system, at least, the Federal Circuit notes because China is a member of the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS), the court “cannot discern any relevant difference between the misappropriation requirements of TRIPS article 39 and the principles of trade secrets law applied by the administrative law judge in this case.”

3. corporate trade secret policy

After discussing the trade secrets laws in Taiwan, China, and the United States, this paper will now offer some suggestions on designing a company's trade secret policy.

When designing a trade secret policy, a company must keep in mind that the purposes of the policy are (1) to minimize the risk of losing trade secrets due to unauthorized disclosure and (2) to demonstrate that reasonable efforts have been taken by the company to safeguard its trade secrets.

3.1 Employee Education

As suggested by the U.T.S.A., a company is advised to inform employees of the existence of trade secrets. The existence of trade secrets and an employee's duty to protect them should be clearly stated on the employment contract. In addition, an employee shall be required to take safety measures regarding the trade secrets, such as restricting off-site access and applying password protection.

Through training sessions, a company can assist its employees in developing good habits on protecting its trade secrets. These habits may include placing "confidentiality" legend on documents containing sensitive information,
erasing whiteboard after discussion, shredding unused documents and destroying unused files, using personal identification code for copying and scanning, reporting suspicious behaviors of co-workers, and not taking documents containing sensitive information outside of the designated area.

3.2 Employee Management

When a company first hires an employee, the employment agreement shall include a confidentiality clause, which prohibits the employee from disclosing the company's trade secrets and other confidential information during and after the employment. The employee shall be given reasonable time to consider the employment agreement and shall be advised to seek advice from personal counsel. Even after the employment agreement has been signed, the company shall regularly remind its employees their duty under the employment agreement, for example, by asking them to acknowledge their duty at the end of an annual training session.

When the employment relationship terminates, the company shall conduct an exit interview, reminding the departing employee about the duty to maintain confidentiality, and about information deemed as trade secrets by the company. Moreover, a company shall ask the departing employee's future career plan, if any, and shall ask whether the employee is still in possession of any company property or file.

In some cases, adding a noncompete clause in the employment agreement may help a company preserving its trade secrets, since competitors are less likely to obtain the trade secrets from the company’s ex-employee. However, a noncompete clause must be properly drafted to ensure its legality. The requirement and enforceability of a noncompete clause differ from jurisdiction to jurisdiction. For example, a noncompete clause is not enforceable in California, but is generally enforceable in Taiwan, China, and most states in the United States.
In general, the territory, the duration and the scope of activity prescribed by the noncompete clause must be reasonable. The reasonableness depends on many factors, such as the ex-employee's position, access to trade secret, the level of competition, and the company's business model.

3.3 Security Measures and Information Technology

It is crucial that a company guards its trade secrets properly. Documents containing trade secrets shall be locked and access to which shall be restricted and recorded. Sensitive files shall be password-protected and stored on a protected network. For places storing a company's trade secrets, access must be restricted.

Furthermore, an automatic log shall be kept for copiers and scanner to record the activity. The log may include the identity of the person requesting the copying, the timing of the activity, the number of pages copied, and page images randomly sampled. Moreover, employees shall be required to change their personal passwords regularly and the complexity of the password shall be specified.

In addition, a visitor shall be required to sign a nondisclosure agreement and shall wear the visitor's badge at all time. If the visitor needs to visit a place exposed to the company's trade secret, proper written approval must be sought and the visitor must be escorted by a designated employee. Finally, all visitor information shall be recorded, but the logbook shall not be placed in public.

4. Conclusion

To gain competitive advantage, a company needs to optimize its intellectual capital through the protection of intellectual property. This requires the company to guard its trade secrets through trade secret laws and a robust trade secret policy. This paper has presented the trade secret laws in Taiwan, China, and the United States. It has also offered some suggestions on designing the trade secret policy on employee education, employee management, and proper security measures and
information technology.


2 35 U.S.C. § 101 “Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.”

3 35 U.S.C. § 271(a) “Except as otherwise provided in this title, whoever without authority makes, uses, offers to sell, or sells any patented invention, within the United States, or imports into the United States any patented invention during the term of the patent therefor, infringes the patent.”


5 Article 2, Trade Secrets Act, Taiwan.

6 *Id.*

7 *Id.*

8 *See* Trade Secret Act § 11, Taiwan, “If a trade secret is misappropriated, the injured party may request for the removal of such misappropriation. If there is a likelihood of misappropriation, a remedy may be requested.” (translation offered by Taiwan Intellectual Property Office); Civil Code § 184, “A person who has intentionally or negligently infringe the rights of another must compensate the caused damages.” (translated by author).

9 *See* Criminal Code § 342, “A person who … acts contrary to his duties and thereby causes damages to the property, or other interest, of the principal shall be punished with imprisonment for not more than five years….” (translated by author); Criminal Code § 317, “A person who is required by law or contract to preserve the commercial secrets of another, who knows or possess such secrets through his employment, and who wrongfully discloses such secrets shall be punished
with imprisonment for not more than one year, detention, or a fine of not more than 1,000 yuan.”
(translated by author); Criminal Code § 318-1 “A person who wrongfully disclose another’s secret
that is known or obtained by the person through the use of computer or other related equipment
shall be punished with imprisonment for not more than two year, detention, or a fine of not more
than 5,000 yuan.” (translated by author).

11 Id.
12 Id.
13 See Benjamin Bai & Guoping Da, Strategies for Trade Secrets Protection in China, 9 NW. J.
14 As of April 2012, only Massachusetts, Texas, North Carolina and New York have not enacted the
U.T.S.A; The Act’s enactment status is available at
16 Id. at §1(2).
17 Id.
18 See E. I. du Pont de Nemours & Co., Inc. v. Christopher, 431 F.2d 1012 (5th Cir. 1970), cert. den.
19 Id.
1207 (7th Cir. 2006) (applying the Wisconsin UTSA).
21 U.S.T.A. §1 comment.
22 Id.
24 See Milgrim on Trade Secrets §1.01; Bond v. PolyCycle, Inc., 127 Md. App. 365, 732 A.2d 970,
972-979 (1999); Abbott Redmont Thinlite Corp. v. Redmont, 324 F. Supp. 965, 969, 971 (S.D.N.Y.
25 U.T.S.A. §2(a)
26 Id.
27 Id. at (c).
28 U.T.S.A. §2(c) comment.
29 See U.T.S.A. §2(b); Republic Aviation Corp. v. Schenk, 152 USPQ 830 (N.Y.Sup.Ct.1967).
30 U.T.S.A. §3(a); Tri-Tron International v. Velto, 525 F.2d 432 (9th Cir. 1975).
31 U.T.S.A. §3(a).
32 Id. at (b).
35 See id.
38 18 U.S.C. § 1839(3).
41 See id.
42 TianRui at 1332-33.
44 See David W. Quinto & Stuart H. Singer, Trade Secrets: law and practice, 202-263 (2009) (listing a comprehensive safety measures a company can take to protect its trade secret).
45 See U.T.S.A. §1 comment.
Rptr. 3d 282 (2008).

47 DeSantis v. Wackenhut Corp., 793 S.W. 2d 670 (Tex. 1990), cert. denied, 498 U.S. 1048 (1991);