June 19, 2009

Discussion of Trade Secrets Protection Posed by Computerization

Sheng-Chen Tseng

Available at: https://works.bepress.com/sheng_chen_tseng/2/
Discussion of Trade Secrets Protection Posed by Computerization

Sheng-Chen Tseng

E-mail: shengtseng1022@yahoo.com.tw
mailing Address: 11666 Summit Cres, Delta, V4E2Z5, BC, Canada
Home number: 604-594-8473
Cell phone number: 778-389-3928

Professor, the Graduate School of Finance & Economic, Ling-Tung University(Taiwan).

Member of Committee in the Intellectual Property Rights Protection of Taiwan Educational Section.

Visiting Scholar & Post Doctor Research Fellow, The University of British Columbia(Canada).
Abstract

The amendment of Taiwan Trade Secret Act has not been implemented for economic espionage crimes and new types of technologies. Thus this paper indicates the suggestion for legislation after analysis of United States laws and Taiwan status quo.

The purpose of the trade secret protection is to maintain industrial ethics and order in competition, encourage the invention and innovation of technologies. Taiwan has regarded the trade secret as a part of the intellectual property. The TRIP Agreement has a great influence on the Taiwan legislation, and other foreign precedents are also taken as the important reference for the Taiwan legislation.

This paper presents the provisions for Taiwan legislation of trade secret protection, the study of USA legislation, and analysis trade secrets protection posed by computerization, and suggestions for Taiwan legal system. The protection of confidential information can promote the R&D and pursuit of profits.

Keywords: Intellectual Property Rights, Trade Secret, Internet, Economic Espionage, Computerization
# Table of Contents

**Introduction** ...................................................... Error! Bookmark not defined.

I. Review for Trade Secret Legislation in Taiwan..............................................5
   1. Trade Secret Act ........................................ Error! Bookmark not defined.
   2. Other relevant laws ..................................... Error! Bookmark not defined.

II. Provisions of relevant U.S laws .....................................................................13
   1. Trade secret and unfair competition ........................................ Error! Bookmark not defined.
   2. Freedom of Information ........................................ Error! Bookmark not defined.
   3. Economic Espionage Act ........................................ Error! Bookmark not defined.

III. Risks to trade secret protection posed by computerization........ Error! Bookmark not defined.
   1. Internet increases the channels for disclosure of secret information .......... Error! Bookmark not defined.
   2. Increasing cost for training and security ......................................... Error! Bookmark not defined.
   3. Importance of Business Strife Limitation Clause and Confidentiality Agreement ........................................ Error! Bookmark not defined.
   4. Summary ........................................................................ Error! Bookmark not defined.

IV. Suggestions for trade secrets protection posed by computerization in Taiwan (Conclusion) ........................................ Error! Bookmark not defined.
   1. Operation Strategies ........................................................................31
   2. Intellectual Property Rights ................................................ Error! Bookmark not defined.
   4. Summary ........................................................................ Error! Bookmark not defined.

References ........................................................................ Error! Bookmark not defined.
Introduction

With the rapid development of information technology, the computerization society results in disclosure and theft of secret information. Thus, how to utilize the convenience of technological tools and internet and meanwhile protect trade secret which is regarded as the vitals of enterprises is worth considering and discussion.

The trade secret is an efficient instrument for survival and development of industrial circles. The industries spare no effort to protect trade secrets. In order to gain competition advantages, enterprises spend significant cost in research to achieve material and immaterial results such as manufacturing method, formula, blueprint, design drawing, customer lists, specification, machine operating method, manufacturing process, plant management practice, and technical records. If this trade secret is disclosed or acquired by rivals, the competition advantages are lost.

Due to the trade secrets have high commercial value, and is the efficient instrument in industrial competitions. Each country formulates the laws to protect the trade secrets so as to maintain the industries operation under the normal competition order, encourage the industrial research and innovation, promote industrial development, and prevent undermining and unfair competition means adopted by commercial espionage to obtain the latest commercial information.

Although the Taiwan Trade Secret Act was promulgated on 17 January 1996\(^1\), the amendment\(^2\) has not been carried out for the punishment of economic espionage and the updated science and technology patterns. Thus this paper presents the suggestions for reference after analysis of USA legislation and Taiwan status quo.

This paper presents the provisions for Taiwan legislation of the trade secrets protection posed by computerization and introduces the USA legislation for the intellectual property rights, especially trade secrets, which exercises a great influence on Taiwan. Thus it is necessary to introduce the USA legislation. Party III will analyze the impact of computerization on trade secrets protection. Finally, the relevant suggestions are raised for the Taiwan legislation.

---

\(^1\) See further description.

\(^2\) Intellectual Property Office, Ministry of Economic Affairs prepared the report and raised suggestions relevant to the amendment of Trade Secret Act, but to date there is no amendment version, see IPO website. http://www.tipo.gov.tw (search date: Aug. 12, 2007).
I. Review for Trade Secret Legislation in Taiwan

The purpose of the trade secrets protection is to maintain industrial ethics and order in competition, encourage the technology invention and innovation, and provide the better consumption environment and choice for consumers. Trade secret protection means to protect the trade secrets from improper disclose or misappropriation so as to encourage technical innovation.

In order to make consistent with and respect the international consensus, Taiwan has regarded the trade secret as one part of the intellectual property. The TRIP Agreement has a great influence on the Taiwan legislation, and other foreign precedents are also taken as the important blueprint for the Taiwan legislation. In the Articles 2, 6, 7, 11 and 12 of the Trade Secret Act, the articles are codified based on concept of rights. All the countries protect the trade secrets subject to the unfair competition prevention law or by other special legislation. In these laws, the trade secret is not clearly defined as right or “trade secret right”, and originally it should belong to an interest. In Taiwan, it is defined as a right due to the policies of legislation. Since the trade secret is defined as the right in the legislation policies, this paper considers the trade secret should be referred to as trade secret right.

World Trade Organization’s TRIPS Agreement prescribes undisclosed information in Article 39, Section 7, Part II. The trade secret protection is included in the Article 39 pertaining to Protection of Undisclosed Information. In the prescription, all the number countries should protect the undisclosed information to prevent unfair competition (Article39 (1)) and further specify the natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information (Article39 (2)).

The TRIPS Agreement clearly requires the member countries to protect the trade secret by laws. In view of the current industrial competitions and economic environment, reference to foreign precedents, conforming to the global trend, due to the pressure of Section 301 of the Trade Act, Trade Secret Act was

---

4 Article 39(2) of TRIPS Agreement in GATT Uruguay Round provides Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information: 1) 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; 2) has commercial value because it is secret; and; 3) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret. This information must (1) be secret (2) have commercial value because it is secret (3) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret. See Luo, C.H., Trade Secret Protection under TRIPS Agreement on, Fair Trade Quarterly, Vol. 4, Issue 3, pp.61-62, July 1996.
5 Before now, Taiwan legislation of trade secret law is the predation for joining GATT. In addition, United States impose the pressure under the article 301 of Trade Act, and the request from information enterprises. In June 15, 1992, United States and Taiwan signed memorandum of
promulgated by Taiwan on 17 January 1996. The Act provides the definition of trade secret, infringement, civil remedies, and methods of calculating damage, and is comprised of 16 articles.

1. Trade Secret Act

Since the Act was enacted in 1996, the substantive rule can be applied to the case of improper theft or leak of trade secret, but there is no division of rights and responsibilities and stipulation of penalties. Thus the trade secret cannot be fully protected. In practice, the current act has deficiencies. The substantive rules and practice views of the Trade Secret Act are as follows:

(1) Contents

The Article 1 of the Trade Secret Act prescribes the legislation purpose: “protect trade secrets, maintain industrial ethics and order in competition, and balance societal and public interests,...” ; reference to foreign legislation, the Article 2 provides: the term "trade secret" as used in this Act shall mean any method, technique, process, formula, program, design, or other information that may be used in the course of production, sales, or operations, and also meet the following requirements: 1) it is not known to persons generally involved in the information of this type; 2) it has economic value, actual or potential, due to its secretive nature; and; 3) its owner has taken reasonable measures to maintain its secrecy.

The Trade Secret Act is applied to the dispute settlement arising from trade secret ownership, which is prescribed in Articles 3, 4 and 5. The Article 3 prescribes the ownership of a trade secret from employment, and the Article 4 provides the ownership of a trade secret from a funded contract. It seems that the ownership of the trade secret is clearly stipulated. However, as for the employment relationship, the Articles 3 prescribes the trade secret is the result of research or development by an employee other than during the performance of employment. The trade secret belongs to the intellectual property and is the

understating, Article 2-10 Understanding Between the Coordination Council for the North American Affairs and the American Institute in Taiwan. The authorities represented by CCNAA will ensure that the industrial design, semiconductor chip protection and trade secret laws meet the standards and requirements of the TRIPS text. The authorities represented by CCNAA commit to use best efforts to work with the LY for the passage of the industrial design law, the semiconductor chip protection law, and, if necessary, the trade secret law, as early as possible, but not later than the LY session ending July 1994.

The Article 3 of the Trade Secret Act provides: If a trade secret is the result of research or development by an employee during the performance of employment, the trade secret shall belong to the employer unless otherwise provided for in a contract, and in which case the contract shall prevail. If a trade secret is the result of research or development by an employee other than during the performance of employment, the trade secret shall belong to the employee. However, if the trade secret is the result of utilizing the employer's resources or experience, the employer may make use of such a trade secret in the employer's business after paying a reasonable compensation to the employee.

The Article 3 of the Trade Secret Act provides: Where one provides funding and contracts another to conduct research or development that resulted in a trade secret, the ownership of the trade secret shall be determined by the terms of the contract. If the ownership is not specified in the contract, the trade secret shall belong to the contracted party; however, the contracting party shall be entitled to make use of such trade secret within the contracting party's business.

6

The Article 3 of the Trade Secret Act provides: If a trade secret is the result of research or development by an employee during the performance of employment, the trade secret shall belong to the employer unless otherwise provided for in a contract, and in which case the contract shall prevail. If a trade secret is the result of research or development by an employee other than during the performance of employment, the trade secret shall belong to the employee. However, if the trade secret is the result of utilizing the employer's resources or experience, the employer may make use of such a trade secret in the employer's business after paying a reasonable compensation to the employee.

7

The Article 3 of the Trade Secret Act provides: Where one provides funding and contracts another to conduct research or development that resulted in a trade secret, the ownership of the trade secret shall be determined by the terms of the contract. If the ownership is not specified in the contract, the trade secret shall belong to the contracted party; however, the contracting party shall be entitled to make use of such trade secret within the contracting party's business.
intangible property right. The proviso of the Article 3(2) provides: however, if the trade secret is the result of utilizing the employer’s “resources or experience”…, how to define the “resources or experience”? The Article 6 of the Trade Secret Act prescribes “a trade secret may be assigned in whole or in part, or jointly owned”; the Article 7: “an owner of a trade secret may grant a license to another for the use of the trade secret. The territory, term, contents, methods of use or other matters in connection with the license shall be determined by the contract between the parties"; the Article 8 provides: “a trade secret shall not be used as the subject matter of a pledge or compulsory execution.” The crime and punishment of economic espionage, civil remedies and damages has not been specified.

The Article 10 (1) of the Trade Secret Act refers to the German and Japanese legislation precedents. The detailed examples constitute the infringement acts, if there are other acts, the remedies can be requested in accordance with the Article 11 of the Trade Secret Act. The Article 9 of the Trade Secret Act ad hoc specifies the confidentiality duty. The policy decided not to specify the article of criminal punishment at the beginning of drafting the Trade Secret Act. In other words, there is no special provision of criminal remedy. The criminal responsibilities of infringement of trade secret are specified in the Articles 316, 317 and 318 of the Criminal Law and the Article 36 of the Fair Trade Act. Only the civil remedies are specified for the infringement of trade secret. As for the civil remedies, the Article 11 of the Trade Secret provides “the injured party may request for the removal of such misappropriation. If there is a likelihood of misappropriation, a prevention may be requested”, the Article 12 provides the right to claim damages, and the Article 13 specifies the methods of calculating damages.

(2) Deficiencies

In recent years, the information dissemination via internet is very rapid, including the email which is convenient and quick, and the trade secret is easier to be leaked. For example, in 2001, the chairman of UMC, Bob Tsao issued the open letter to his employees via email, and the letter was disseminated throughout the same trade in one hour. In this case, regardless of whether this

---

8 The trade secret is different from the rights such as copyright, trademark right, and patent right, for the discussion of the ownership of copyright and patent right, see Hsieh, M.Y., “Ownership and Management of Intellectual Property Right—including Relevant System in Germany”, Basic Theory of Intellectual Property Right, pp.93-117, 1995; Chen, W.Y., Discussion on Patent Law, pp.128-132, Oct. 1997.

9 (1) provides: any use or disposition of a jointly-owned trade secret shall be unanimously approved by all co-owners in the absence of a contractual provision; however, no co-owner shall refuse consent without proper justification (2); no co-owner may assign its share of the ownership without the consent of the remaining co-owners, unless otherwise provided for in a contract, and in which case the contract shall prevail (3).

10 (1) provides: the licensee as referred to in the preceding Paragraph shall not sub-license the licensed trade secret without the consent of the trade secret owner; (2) no co-owner shall grant a license to another for the use of the jointly-owned trade secret without the unanimous consent of the remaining co-owners; However, no co-owner shall refuse consent without proper justification (3).

11 Bob Tsao issued open letter in July 2, 2001. After the disclosure is reported by media, the
matter leaked the trade secret, it is indisputable email is the popular way to disseminate the information in industries. How to ensure the security of dissemination and prevent the data leak make the division of rights and responsibilities and criminal liabilities necessary. The criminal punishment is not specified in the Trade Secret Act. Although some relevant criminal cases can be applied to the Criminal Law or the Fair Trade Act, there is no special regulation to divide the rights and responsibilities and criminal liability. Both the Criminal Law and the Fair Trade Act have the obvious deficiencies.

Taiwan Trade Secret Act refers to the infringement acts in the German and Japanese unfair competition prevention laws. To use or disclose by improper means a legally acquired trade secret, such as employment, commission, proxy, contracting and authorization, which cause the damages to the owner of the trade secret, should be prohibited. As for the prohibition of business strife, the government employees and other parties related use or disclose without due cause any trade secrets of others, known or obtained by virtue of a judicial investigation or proceeding, shall be punished under the Trade Secret Act.

The commercial espionage proves the trade secret leak can impact the competition. The injured party—whether individual or corporation—invested in research and development and production, which indirectly impact the investment willingness and increase the wasting of social resources. In addition to division of the liability of the party concerted, it is important to effectively prevent the infringement of the trade secret.

Taiwan formulates the special law not to crack down on the economic espionage but also severely punish the transnational theft of trade secret. The subjects include the Taiwanese and foreign persons. Taiwan laws have the deficiencies in the punishment of economic espionage, and the effect of the civil remedies has limitation. If the procedure is slow or the there is no way of remedies, the infringement of the trade secret cannot be effectively protected.

2. Other relevant laws

Before promulgation of Trade Secret Law in the 1996, the relevant disputes were settled in accordance with other laws or legal theory, including the Civil Code, Corporate Law, Fair Trade Law and Criminal Law.

(1) Civil Code

To acquire a trade secret by trust or inducement of others to breach the trust is deemed as the manner against the rules of honesty and morals; or to acquire a trade secret by attracting an employee of an opponent, which infringes the obligatory right of others shall be punished according to the last paragraph of Article 184(1) \(^{12}\). For example, a person discloses without due cause any trade

---

\(^{12}\) The last paragraph in the Article 184 (1) of the Civil Code: “A person who, intentionally or negligently, has wrongfully damaged the rights of another is bound to compensate him for any injury arising therefrom. The same rule shall be applied when the injury is done intentionally in a manner against the rules of morals. A person, who violates a statutory provision enacted for the protection of others and therefore prejudice to others, is bound to compensate for the injury,
secrets of others known or obtained through business according to the ordinance or the contract; government employee discloses without due cause any trade secrets of others known or obtained through the performance of his official duties; a person deals with the affair of others for his own or third-person's illicit profits, or infringes his own interest to breach his duty, which infringes his property or other interests. These above infringement acts of trade secret are illegal due to violation of the provisions above, according to the last paragraph in the Article 184 (1) of the Civil Code, a person, who violates a statutory provision enacted for the protection of others and therefore prejudice to others, is bound to compensate for the injury. A manager or commercial agent shall not without the consent of his firm enter on his own account or on account of third parties into any business of the same kind as that which he is commissioned for his firm, nor can he be a partner with unlimited liability in a commercial firm which carries on the same kind of business. On May 23, 2007, the Articles 562 and 563 of the Civil Code were amended, which is supplementary to competition prohibition articles for a manager or commercial agent.

(2) Corporate Law

Articles 32, 54, 108, 115, and 209 of the Corporate Law prescribe the he

---

13 Article 317 of the Criminal Law.
14 Article 318 of the Criminal Law.
15 Article 342 of the Criminal Law.
16 Article 562 of the Civil Code: “a manager or commercial agent shall not without the consent of his firm enter on his own account or on account of third parties into any business of the same kind as that which he is commissioned for his firm, nor can he be a partner with unlimited liability in a commercial firm which carries on the same kind of business.”
17 Article 563 of the Civil Code: “if an action of a manager or commercial agent violates the provisions specified in the preceding article, his firm may demand from him, as the injury, the profits resulting from his act. The right to claim under the preceding paragraph is extinguished by prescription if it is not exercised within two months from the time when the firm knew of the violation or within one year from the date of the act.”
18 Article 32 of the Corporate Law: “a managerial personnel of a company shall not concurrently act as a managerial personnel of another company, nor shall he/she operate, for the benefit of his/her own or others, any business which is the same as that of the company employs him/her, unless otherwise concurred in by the company pursuant to the provisions of Paragraph One, Article 29 hereof.” Article 54 (prohibition of business strife and disgorgement of corporate): “a shareholder, without the unanimous consent of all other shareholders, shall not be a shareholder of unlimited liability of another company or a partner in a partnership business; a shareholder who conducts business of the company, shall not, on his own account or on behalf of another, engage in the same business as that of the company; if a shareholder who conducts business of the company violates the company on his own account or on behalf of another, he shall not at the same time represent the company; however, the repayment of debt to the company shall be excepted.” Article 108(3): “where a director intends to conduct, for the benefit of his/her own or others, a business of the same kind as that of the company, he/she shall make an explanation to all shareholders about the important contents of such act and shall obtain a prior consent of a majority of all shareholders.”; Article 115: “the provisions of Chapter II shall mutatis mutandis apply to an unlimited company with limited liability shareholders unless otherwise provided for in this chapter.”; Article 209 (prohibition of directors’ business strife and disgorgement of corporate): “a director who does anything for himself or on behalf of another person that is within the scope of the company’s business, shall explain to
competition prohibition for shareholders and directors so as to protect trade secrets. For example, the Article 48 of this Law provides Shareholders who do not conduct business may, at any time, require shareholders who conduct business to furnish information on the business condition of the company and examine its assets, documents, books and statement. Thus the corporate trade secret is not the secret to the shareholders. If they carry out the same kind of business, the corporate will be infringed. However there is no restriction on them. The prohibition of business strife only applied to the protection of trade secrets when the managers, directors, shareholders and commercial agents are in office or have the titles. However many infringements happened when they are out of office. Thus the above provisions cannot protect the parties related to the trade secrets.

(3) Fair Trade Law

The Fair Trade Law was announced on February 4, 1992 for the purpose of “maintaining trading order, protecting consumers' interests, ensuring fair competition, and promoting economic stability and prosperity.” The Trade Secret Act was promulgated on January 17, 1996 to “protect trade secrets, maintain industrial ethics and order in competition, and balance societal and public interests”. Both of the laws are enacted to balance societal and public interests. The difference between the Trade Secret Act and the Fair Trade Law is that the Trade Secret Law is applied to the broader subject range, protection range and wrongful acts.

The Article 19(5) of the Fair Trade Law forbids the acquiring the trade secret by improper means and protects the subject of the trade secret ownership, only limiting to the "enterprise" set out in the Article 2 of this Law, including a company, a sole proprietorship or partnership, a trade association, any other person or organization engaging in transactions through the provision of goods or service, and also including the "trading counterpart" set out in the Article 2 of this law means the any supplier or purchaser that engages in or concludes transactions with an enterprise, not the natural person engaging in research and invention.

Therefore the Fair Trade Law has the deficiency for the infringements. This Law protects the trade secret of enterprises, and only punishes the infringement of the enterprises' trade secret (the Article 2 of the Trade Secret Law). The trade

the meeting of shareholders the essential contents of such an act and secure its approval”.

19 Article 19(5) of the Fair Trade Law: acquiring the secret of production and sales, information concerning trading counterparts or other technology related secret of any other enterprise by coercion, inducement with interest, or other improper means. The trade secret in this Article should meet at least two requirements according to the views of the Fair Trade Commission (1) secretive nature, the disclosed or the known knowledge or technologies are not the objects protected in the Article 19(5) of the Fair Trade Law, in addition, owner of the secret has taken reasonable measures to maintain its secrecy and prevent others from knowing it. (2) it has economic value: acquisition of the trade secret can obtain the competition advantages. Understanding Fair Trade Law (8th revised and enlarged edition), pp.186-187, August 2001. See Feng, C.Y., Discussion on Relationship between Trade Secret Law and Competition Law – including the Application of Article 19 (1) (v) of Fair Trade Law, Fair Trade Quarterly, Vol. 4, Issue 3, pp.1-38, March 1996.
secret of the natural person is not protected by the Fair Trade Law. Thus the protection provision of the Fair Trade Law can not fully ensure the fair competition and maintain the commercial ethics.

The criminal punishment and administrative punishment are not implemented for the first infringement of the trade secret, and the Fair Trade Commission only orders to cease the conduct\textsuperscript{21}. In accordance with the Article 19(5), object for protection is the “secret of production and sales, information concerning trading counterparts or other technology related secret,” and the content and the scope of the trade secret is not defined. In terms of interpretation, the protection scope should be limited to the “technology related secret.” The protection scope is narrower than the scope of the Trade Secret Law.

As for the infringements, the unlawful acquiring is deemed as the object of punishment. But some acquiring is more censurable, the “unlawful disclosure” and “improper use” have not been constituted a sanction pursuant to this Law, which may impair the fair competition. The acquiring of technology related secret not for competition is not deemed as the object of punishment. The unfair competition has the nature of the unfair competition such as failing to obey the other articles of this Law, and whether the Article 24 of this Law applies. The so called unfair competition is censored for the violation of the commercial competition ethics. In other words, such violation of the social ethics or infringement of the nature of the fair competition based on price, quality and service is the unfair competition. If any enterprise infringes the trade secret, which meets nature of the unfair competition, the Fair Trade Commission can supplement the deficiency of the Article 19(5) through cases and interpretation. To date, there is no relevant case for reference.

(4) Criminal Law

The violation of trade secrets can be deemed as the disclosure of business secrets and computer or equipment related secrets, theft, misappropriation and breach of trust pursuant to the Criminal Law, but no special chapter discusses the disclosure of trade secrets. Any person discloses without due cause any business secrets of others know or obtained through business according to the ordinance and contract\textsuperscript{22}; any government employee or former government employee discloses without due cause any business secrets of others know or obtained through the performance of his official duties\textsuperscript{23}; any person discloses without due cause any business secrets of others known or obtained through the computer or other equipment\textsuperscript{24}. In principle, the object of theft is the tangible

\textsuperscript{21} See Article 36 and 42 of the Fair Trade Law.
\textsuperscript{22} Article 317 of the Criminal Law: “any person disclosing without due cause any business secrets of others know or obtained through business according to the ordinance and contract shall be punished by imprisonment for not more than one year or detention, or fined of not more than one thousand New Taiwan Dollars.”
\textsuperscript{23} Article 318 of the Criminal Law: “any government employee or former government employee disclosing without due cause any business secrets of others know or obtained through the performance of his official duties shall be punished by imprisonment for not more than two year or detention, or fined of not more than two thousand New Taiwan Dollars.”
\textsuperscript{24} Article 318-1 and 318-2 of the Criminal Law: “any government employee or former government
object. If the trade secret is attached to tangible object, the actor acquires the secret unlawfully, which constitutes the theft. If the trade secret is attached to the tangible object, actor intends to misappropriate the tangible object for his own or third-party interests, this constitutes the misappropriation crime. Aggregated punishment is given to the person acquires the secret through official duties, public welfare or business.

More than that, any person intends to deal with affairs of others for his or third person interests, or infringing his own interest for breach his duty, causing damages to his own or third person property constitute breach of trust. The employees may disclose the corporate secret known through the performance of employment, to the opponent.

(5) Deficiency

i. Civil Code: a) if the remedies are requested due to tort act, the “virtuous mores” set forth in the Code is not explicit, only the indemnity for damage can be requested, no nonfeasance right of claim; b) request for contractual liability requires the contractual relationship between parties.

ii. Corporate Law: the prohibition of business strife can not restrict the dimission.

iii. Fair Trade Law a) the protected object of the Fair Trade Law is only limited to the trade secrets of “enterprise”, other trade secrets which not belong to the “enterprise” will not be protected; b) under the important conditions of the criminal punishment and administrative punishment, the first infringement of trade secret is not punished; c) the protected object is the “secret of production and sales, information concerning trading counterparts”, the content or the scope of the trade secret is not defined, the protected scope is narrower than Trade Secret Act; d) only the unlawful acquiring is deemed as the object of punishment.

iv. Criminal Law: a. the violation of the trade secret is punished as theft and misappropriation crime, based on the doctrine of a legally prescribed punishment for a specified crime, many vicious acts, such as, the employee copies the confidential file without permission, can not be punished. b. under the provisions of patent law, the action subject of the theft of commercial secrets or breach of trust, take a certain status as a actor, if no this status, no basis for punishment, and thus the Criminal Law has the inadequacy for the employee disclosing without due cause any business secrets of others know or obtained through the performance of his official duties shall be punished by imprisonment for not more than two year or detention, or fined of not more than two thousand New Taiwan Dollars.

---

25 Article 320 of the Criminal Law: “any person intending to steal the movable property of others for himself or third-person, constitute theft crime, and shall be punished by imprisonment for not more than five year or detention, or fined of not more than five hundred New Taiwan Dollars. Any person intending to misappropriate the movable property of others for his own or third person interests shall be punished pursuant to the preceding paragraph; Article 323: “electric energy, thermal energy and other energies, the crimes in this chapter are involved in movable property.

26 Article 335 to 338 of the Criminal Law.

27 Article 342 of the Criminal Law: “any person intending to deal with affairs of others for his or third person interests, or infringing his own interest for breach his duty, causing damages to his own or third person property shall be punished by imprisonment for not more than five years or detention, or fined with not more than one thousand New Taiwan Dollars, or both.”
II. Provisions of relevant U.S laws

In American laws, some are federal acts, some are state laws. In order to protect trade secret and prevent the economic espionage, the relevant contents and the resolution of doubts about the applicability of trade secrets protection posed by computerization are described as follows. The discussion can be divided into trade secret and unfair competition, freedom of information and economic espionage.

1. Trade secret and unfair competition
The Uniform Trade Secret Act, Restatement of Unfair Competition, and Restatement of Torts are described as follows.

(1) Uniform Trade Secret Act

Before the enforcement of Economic Espionage Act in 1996, the basic principles of common law trade secret protection was codified in the Trade Secret Act. American Bar Association drew up the Uniform Trade Secrets Act (UTSA)[28] in 1996. Afterwards, the association founded the National Conference of Commissioners on Uniform State Laws to adopt the UTSA in August 9 in 1979.

In order to federalize the protection of trade secret and proprietary information, the trade secrets protection is specified in the statute law[29]. In June 1948, the Trade Secrets Act (TSA) was constituted. Afterwards, TSA was amended to punish the infringement of personal trade secret[30]. TSA can protect the financial data of bank, but cannot assist the parties in the civil proceeding to prevent the disclosure of the relevant data. In addition, the content protected by the TSA is also protected by the (the Freedom of Information Act (FOIA). TSA is a model law for trade secrets protection and is observed by the employees or commercial agents[31].

After 1980, the states adopted “Uniform Trade Secrets Act”[32] proposed by American Bar Association, and recognized and protected trade secrets. However the states held different theoretical bases, the protection extents are also different. This causes problems for many corporations and industries. The Uniform Trade Secrets Act provides the civil remedies. However the actual damages resulted from the infringement of trade secret, or malice for the theft of trade secrets and the theft crime has not been effectively prevented. Uniform Trade Secrets Act is the important reference for legislation of state-based laws of trade secrets[33].

---

[30] 18 U.S.C. §1905 (2000), the violators may be punished by a fine or by imprisonment for not more one year.
(2) Restatement of Unfair Competition

This restatement\(^{34}\) prescribes the liability for improper appropriation of trade secrets. In other words, if the natural person acquires the secret from a third person, irrespective of the natural person knew or did not know the secrecy of the information, he is not punished except for scienter or malignance. If the natural person did not know or cannot know the information is trade secret, he bears no liability until he knows it is trade secret and continues to use it\(^{35}\).

Before now, the unfair competition theory was applied to the protection of trade secret or confidential information, see the Restatement (First) of Torts §759\(^{36}\) “[o]ne who, for the purpose of advancing a rival business interest, procures by improper means information about another’s business is liable to the other for the harm caused by his possession, disclosure or use of the information.” The theoretical basis for the determination of the liability of parties is acquiring and use of the property of parties and competitive behavior\(^{37}\). The purpose of the legislation is to avoid the theft or misappropriation without authorization, the object of the crime is not always the trade secret.

Restatement (Third) of Unfair Competition (1995) defines a trade secret as “any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others.”\(^{38}\) The parties use, steal or disclose the trade secret for the purpose of competing with opponents not simply of increasing profit and commercial opportunities, such as steal the information related to raw materials, ingredients, formula, even the trade method, plan and customer list.

(3) Restatement of Torts

If the Restatement of Torts was adopted before EEA, this is one of main law sources for resolving the litigation on trade secret.

The Restatement of Torts was completed by the American Law Institute in 1939. The section 757 through 759 and comments in chapter 36 define trade secret and describe the type of infringement\(^ {39}\). The definition of trade secret and

---

\(^{34}\) Restatement (Third) of Unfair Competition (1995).


\(^{36}\) Restatement (First) of Torts §759 (1939) & §759 cmt. b.

\(^{37}\) Unikel, supra note 44, at 862-863.


\(^{39}\) According to Restatement of Torts, 757 (1939), Comment b. Definition of trade secret: “A trade secret may consist of any formula, pattern, device or compilation of information which is used in one’s business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it. It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers. It differs from other secret information in a business (see section 759) in that it is not simply information as to single or ephemeral events in the conduct of the business, as, for example, the amount or other terms of a secret bid for a contract or the salary of certain employees, or the security investments made or contemplated, or the date fixed for the announcement of a new policy or for bringing out a new model or the like. A trade secret is a process or device for continuous use in the operation of the business. Generally it relates to the production of goods, as, for example, a machine or formula for the production of an article.
description of the type of infringement has the high reference value. However, this
Restatement of Torts is derived from early case law and was completed in 1939.
Due to the abstract contents, the Restatement of Torts cannot catch up with the
rapid commercial activities. Thus, the American Law Institute adopted the
Restatement of Torts, 2d, 1978. The definition of the trade secret is deleted, but
the definition is often cited by courts, so it is of the jurisprudence value.\textsuperscript{40}

Previously, the disputes on the trade secret were governed by the UTSA and
the Restatement of Unfair Competition, but the Restatement of Torts was often
applied to the disputes. After several amendments, the definition of trade secret
is different from the previous one, but it still includes any process, pattern,
device, formula or any information of a business or other enterprise that can
afford economic advantage over opponents.\textsuperscript{41} The American Law Institute
proposed to “federalize” the law of trade secrets in the intellectual property
meeting in 1992,\textsuperscript{42} but the proposal was not put into practice.

(4) Summary

1. to date, there are 42 states and District of Columbia enact their state law
of trade secrets based on the UTSA,\textsuperscript{43} but the UTSA and the state-based
law of trade secrets have flaws, such as the interstate theft of trade
secrets cannot be effectively prevented, no punishment for foreign
economic espionage\textsuperscript{45} and the crime cannot be prevented.\textsuperscript{46}

\begin{itemize}
\item It may, however, relate to the sale of goods or to other operations in the business, such as a
code for determining discounts, rebates or other concessions in a price list or catalogue, or a
list of specialized customers, or a method of bookkeeping or other office management”. Lin,
C.B., Research on the Concept of Trade Secrets and the Type of Misappropriation, master’s
\item Feng, C.Y., Understanding of Trade Secret Law—Trade Secret Law Theory and Practice, p.309,
1997.
\item Restatement (first) of Torts, 757 c.m. b (1982).
\item This conference was held in San Francisco in 1992, Annul Report, 1992-93 A.B.A. SEC. IPL
300-09, the legislation progress for trade secrets is very slow. Although some federal laws
have the similar stipulations, the issues related to economic espionage cannot be resolved
effectively. For example Communications Assistance for Law Enforcement Act, Pub. L. No.
\item Lin, H.L., Analyses of U.S. \textit{Economic Espionage Act}—including strategies for Taiwanese
employees, master’s thesis, Graduate Institute of Law, Tung Hai University, p.15, June 2000;
more than 40 states have adopted UTSA, the other states still follow Restatement of Unfair
Competition and Restatement of Torts codified by the American Law Institute.
\item The second part of this section will introduce laws related to transportation of stolen property
and fraud, especially the Interstate Transportation of Stolen Property Act of 1934, but this laws
provides the tangible property, and cannot prescribe the intangible property such as trade
secrets.
\item UTSA is United States federal law and is the model law for the state. It is applied to the
domestic infringement of trade secrets, can not bind the offender who is foreigners or foreign
organization. For international justice, the territory has to be considered.
\item EEA deprives the freedom and property of actor, and punishes the offender of conspiracy. Its
criminal penalty is severer than UTSA. In addition EEA was federal law passed by the
Congress, and can replace UTSA which does not cover the foreign economic crimes and
enforcement. The definition of trade secrets in EEA adopts the definition in the UTSA, such as
\end{itemize}
2. the Restatement of Unfair Competition is applied to the circumstance that defendant's acts has constituted unfair competition.

3. the definition of trade secret in Restatement of Torts (1939) has been deleted, but the content is often cited in the American practical field, because it is explicit, reasonable and not confused.

2. Freedom of Information

Free use and exchange of information is the basic right of the people. However the prevention of trade secrets disclosure will restrict the freedom of information. In order to understand the purpose and roles of the legislation, the Electronic Communications Privacy Act (ECPA), Freedom of Information Act (FOIA) and Electronic Signatures in Global and National Commerce Act (ESIGN) are described as follows.

(1) Electric Communications Privacy Act

In this Act, wire communication means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.

The law was passed by Congress in 1986, and Title 18 of the Civil Code provides the unlawful access to stored communications, whoever intentionally accesses without authorization a facility with an electric communication service. However, the computer hacker without authorization or the committing a crime using internet cannot be prosecuted.

Due to the development of the communication media and prevalence of the modern technical tools, the electronic facilities quicken the communication between people. In ECPA, manufacture, distribution, possession, advertising, buying and selling, or transportation of electronic communication intercepting the owner has taken reasonable measures to keep such information secrets, the information have economic value, actual or potential. The definition is broader than UTSA. Unif. Trade Secrets Act, 1(4), 14 U.L.A. 433, 438 (1985) (using language similar to subsections (A) and (B), and providing as examples “a formula, pattern, compilation, program, device, method, technique, or process”), definition of trade secrets in UTSA is more fixed, the definition in EEA is recapitulative, including boarder objects.


48 Under the US Civil Code, the electronic communication include any signs, signals, words, images, voice, data or any expression of thought. If a communication made in whole or in part by wire, radio, or images violates the prescription, means violation of ECPA. Electronic Communications Privacy Act, Legislation, http://legal.web.aol.com/resources/legislation/ecpa.html (last visited 2003/8/17).

49 Id.

50 The Omnibus Crime Control and Safe Streets Act (OCCSSA) was passed in 1968; Pub. L. No. 90-351, 82 Stat. 197 (1968), title III Ecpa (Sec. 605) set rules for obtaining wiretap orders (18 U.S.C. §§1510, 2510-2522, 2701-2709, 3121-3126 (2000)), except the government actions, the background of this legislation is the Fourth Amendment, ECPA prohibits wire and oral communication, expect the agreed disclosure.
devices constitutes the federal crime.\footnote{18 U.S.C. 2511(1)(2000).}

(2) Freedom of Information Act

From 1950 to 1960 the dissemination of the information is rapid, so the congressmen considered it was necessary to adopt the Freedom of Information Act (FOIA).

This Act was enacted in 1966 and was amended several times.\footnote{FOIA, Pub. L. No. 89-559, 80 Stat. 383 (1966) (codified in 5 U.S.C. 552 (2000)).} This act allows for the full or partial disclosure of previously unreleased information and documents controlled by the United States Government. In order to ensure the freedom of information, the government information is available to the public under this act. It also provides eight categories of exemptions\footnote{Under this Act, there are nine exemptions. The right for solicitation of information can be refused, if the information is related to trade secrets or to prevent unfair competition. United States Department of Justice, \url{http://www.usdoj.gov/04foia/index.html} (last visited 2003/8/17).} to ensure appropriate confidentiality of sensitive information; the forth is related to trade secrets which definition is narrower than that of UTSA. The commercial or financial information is protected to some extent. FOIA hopes there are some restrictions to acquire the information but still to ensure the freedom of information, including the judicial procedure.

Under the FOIA, the federal government agencies should provide the relevant information for the person who submits a petition. If the information is “trade secrets and commercial or financial information obtained from a person and privileged or confidential,” the federal government agencies will not disclose the information. The agencies can decide whether or not to disclose trade secrets or confidential information to the applicant according to their authorities. In this act, notifying holders of the information prior to disclosure is not specified. President Reagan issued the Executive Order limiting the FOIA in 1987, and this order specifies the federal agency shall be responsible for notifying holders of the information prior to disclosure.

(3) Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act\footnote{The Computer Fraud and Abuse Act 18 U.S.C. 1030 (2000).} (CFAA) is a law intended to reduce "hacking" of computer systems and to address federal computer-related offenses, especially the malicious dupery. This act is different from the protection of Electric Communications Privacy Act. The data stored in the computer is protected under the CFAA.\footnote{David B. Fein and Mark W. Heaphy, \textit{Companies Have Options When Systems Hacked Same technologies that empower corporations can expose vital proprietary information}, 27 Conn. L. Trib. 5 (Oct. 15, 2001).}

CFAA was passed by the United States Congress in 1984. The accessing a computer without authorization to obtain information contained in a financial record is deemed as criminal offense under this act. The information includes...
credit ratings of customers or the information from the protected computer, which is the object of crime. After legislation of CFAA, fraud or infringement via computer in interstate or foreign commerce constitutes federal criminal offense. CFAA is the first act to punish the crimes in electronic commerce or financial institutions, but exclusive of the increasing computer commercial espionage.

This act is capable of addressing federal computer-related offenses such as fraud or misappropriation via computer, and the civil damages can be claimed under this act. The access computer without or in excess of authorization is the wrongful action under CFAA, the need of this act is very obvious in practice. In recent years, an internet hacker commits a crime via hard stored data of computers. For instance, hacker accessed information on as many as 8 million American Express and Visa and MasterCard credit card accounts, which posed a great threat to the customers.

This Act was amended in 1994. Specifically, it was modified to prohibit not only unauthorized access to a computer system, but also "transmission of a program, information, code or command" that "intentionally causes damage without authorization." Thus, after the 1994 amendment, the CFAA allowed the federal government prosecution for a computer-related crime, and prohibited acquisition of the confidential, financial, and customer-related information of others via computer without authorization. CFAA was no longer limited to protecting computers deemed necessary for national security and the national economy, but instead covered all computer data involved in interstate and foreign commerce, especially involved in electronic commerce business, this Act can effectively crack down the economic espionage.

(4) Summary

1. ECPA limits hindering of privacy of others via electronic communication, the use of electronic communication is not limited in America or foreign commerce, but must be through the telecommunication, radio or electronic channels.

2. FOIA allows the federal government to disclose and control the

---

58 Id.
59 In fact, in addition to this, the commercial espionage is growing in enterprises and industries. Id.
information, lessen the time and costs, focuses on the types of acquisition of domestic information.

3. CFAA limits the computer-related or internet–related crimes to protect the privacy of electric communications.

3. Economic Espionage Act

Economic Espionage Act of 1996 (EEA) internationalize the trade secret protection, and the crimes outside America can be prosecuted. The criminal punishment is applied to the economic espionage activities and theft of trade secrets. The internet can make the information disseminate without limitation, which becomes the optimum tool to disclose trade secrets. The current federal statutes cannot effectively prevent the theft of trade secrets via high technology, and the enterprises only bring a civil suit to request compensation for damages. The severe criminal punishment is imposed on the theft of trade secrets by American government. Before the EEA was passed, each state protects trade secrets by their own laws, though the states follow Interstate Transportation of Stolen Property Act of 1934 (ITSP), the intellectual property cannot constitute the defined “goods”. In the early 1930s, the act was enacted to prohibit interstate transportation of stolen “goods, wares or merchandise”, but exclusive of the stolen information. Thus law is not applied to prosecution of economic espionage.

Most of state-based laws provide the request for damages due to improper disclosure of trade secrets. However, the continuing use cannot be prevented after parties paid the fines, or the parties had gained great interests before paying the fine. Once the trade secret is disclosed, the damages of injured parties

64 R. Mark Halligan, The Economic Espionage Act of 1996: The Theft of Trade Secrets is Now a Federal Crime, http://execpc.com/~mhallign/crime.html (last visited 2000/8/28). The National Stolen Property Act was passed by Congress in 1934, this act prevents the stolen goods transported by vehicles, but the government must prove the stolen goods are goods, wares or merchandise, and the transported goods are stolen, converted or taken by fraud).
65 18 U.S.C. §2314. after cold war ended, the sensitive enterprise information and advanced technical information are threatened increasingly, because foreign governments, no matter they are foes or friends make their resources of espionage activities shift from military and political information to the commercial information. see theft of trade secrets cases in United State, for details, seehttp://www.moeacnc.gov.tw/CNJ/CNJ0603-9006.html (search date: April 20, 2002).
66 Caryl Ben Basat, the Economic Espionage Act of 1996, 31 Int’l Law. 245 (1997), http://web.lexis-nexis.com/universe/document?m (last visited 2007/10/01). This act has the limitation on the amount of protected objects, under subsection 2314, the elements of a violation of the offense are that defendant: 1) takes goods by stealing, fraud or transmission; 2) unlawfully transported or caused to be transported in interstate or foreign commerce; 3) goods, wares, merchandise, securities, or money having a value of $5,000 or more which are stolen; 4) knowing the same to be stolen, converted or taken by fraud. The objects do no have to have a value of over $5,000 USD; most judicial authorities think the law is applied to the tangible objects, not the intangible commercial information. The state-based laws cannot effectively protect trade secrets due to inadequacy of the laws not criminal penalty for infringement of trade secrets, thus the states are difficult to prohibit the interstate or international infringement. See Chang, C.H., Brief Introduction of Economic Espionage Act, Feb. 20, 2002, http://www.copyrightnote.org/crnote/bbs.php?board=8&act=read&id=10 (search date: Aug. 12, 2007).
cannot be remedied. Thus, ITSP cannot be applied to the economic espionage. EEA addresses the economic espionage crimes and provides the punishments.

(1) Economic Espionage Act

Before the enactment of the EEA, the injured parties request for damages caused by economic espionage only through civil suit, this can not prevent the offender from repeated violation of laws and preclude the piracy. Due to the results of criminal and civil compensation are different, the civil code prescribes the liability for such damages, and the criminal laws prevent the crimes in advance to correct the actor behavior. The EEA intends to prohibit the crimes to correct the actor behavior, so it reinforces the criminal penalty and prescribes the act of economic espionage in section 1 and 2. This law provides the espionage actor, the types of activity, contents, including the espionage activity supported by foreign governments and the theft of trade secrets.

The EEA make the theft of trade secrets (who knew or should have known the information is confidential) a criminal act, regardless of who benefits. EEA is not capable of protection of the disclosed trade secret due to negligence or unintention. To prohibit the opponents from enticement of the employees of others to steal important corporate or governmental documents, information or trade secret, the foreign government, foreign instrumentality or foreign agent in EEA 18 U.S.C. §1831 means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed or dominated by a foreign government. Although Taiwan has not established the formal foreign relations with U.S., but the EEA 18 U.S.C. §1831 is applied to Taiwanese personnel in U.S representative office.

(2) Theft of trade secrets

As for a traditional economic espionage, if FBI investigates no foreign government supports him, the 18 U.S.C. §1832 can apply. In other words, the theft is investigated as the domestic theft of trade secrets. After passage of EEA, the federal statutes can more effectively prohibit the espionage activities, the 18 U.S.C. §1831 and 18 U.S.C. §1832 provide the principle of the criminal penalties, §1833 prescribes the exceptions to prohibitions.

---

68 Enterprises often adopt two methods. In the procedure of civil compensation, most of corporations may bind the employees through no-compete clause and confidentiality contract. David Cathcart, Contracts with Employees: Covenants Not To Compete and Trade Secrets, 36 Ali-Aba 87, 100 (1997). If an employee violates the contract, the corporation can sue employees over violation of contracts or fiduciary duty; secondly, corporation can prosecute employee for improper use of trade secrets under the Torts laws. Till date, more than 40 states adopt UTSA, so corporations can request for civil prohibitive injunction or compensation, which is the advantages of civil suit. Jonathan Band, The Economic Espionage Act: Its Application in Year One, Corp. Couns., at 1 (Nov. 1997).


70 Id.


Under Section 1832, the theft of secrets “whoever, with intent to convert a trade secret, that is related to or included in a produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof” is different from foreign economic espionage threatens the national security, the intent of the theft is economic benefit. Thus the Congress requires the Attorney General to prove that defendant intended to obtain the economic benefit and obtained the economic benefit.

For any violations of EEA, any intent to infringe or know infringement benefits a foreign government or agency, is the essential conditions of economic benefit, regardless of whatever merchandise. The implementation of a strategy or the action to be done to benefit a foreign organization can be punished under Section 1831; under Section 1832, the theft of trade secret must be involved in products, and the persecution requirement is higher. The congressional legislation intent is to prohibit the economic espionage activities supported by foreign government, which threatens American security and economy. Compared with the domestic theft of trade secrets, no matter that defendants are American or foreign persons or enterprises, the damages will not threaten America.

(3) Effect

The U.S. Congress enacted the EEA in 1996, which meant to provide the legislation model for other countries to protect trade secrets, in response to rapidly changing world of technology. The enactment demonstrated U.S maintain and protect the economic interests of enterprises. In the following, we discuss the actual benefits of the EEA enforcement.

The commercial and industrial competitions are sharp, and the advanced information technology is the key to success. The intelligence activity is shifted to the theft of U.S economic secrets and intellectual property. These infringe the U.S economic interests, and the federal statutes cannot effectively punish economic espionage. Thus EEA is a powerful weapon to these problems. The Federal Government of the USA prohibits the foreign government or agency from acquisition of USA commercial secrets by improper means especially high tech.

77 December 17,1992, the governments of the United States, Canada, and Mexico created the North American Free Trade Agreement (NAFTA), NAFTA mainly follows United States Trade Secrets Law; in April 15, 1994, General Agreement on Tariffs and Trade was replaced by the World Trade Organization (WTO); the Uruguay Round in 1986 produced the WTO Trade Related Aspects of Intellectual Property Rights (TRIPS) agreement, which defines the undisclosed information. The protection must apply to information that is secret and that has commercial value.
78 The Select Committee on Intelligence, the Judiciary Subcommittee on Terrorism, Technology and Government Information (Senate) and the Subcommittee on Crime of the Judiciary Committee (House of Representatives) are responsible for legislation of EEA. The members who are invited to attend the hearing are not limited to the experts in the field of intellectual property. After review of the previous literature, EEA is often cited by FBI (S. Rep. No. 104-359, at 5 (1996); H.R. Rep. No. 104-788, at 14-16 (1996) testimony of FBI Director Louis J. Freeh.
79 After enactment of EEA, the members of the House of Representatives Tom Davis et al.
The sanction on the economic espionage which benefits foreign instrumentality or foreign agent is very severe.

EEA does not prohibit (1) any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State; or (2) the reporting of a suspected violation of law to any government entity of the United States, or a political subdivision of a State, if such entity has lawful authority with respect to that violation.

The federal government finds USA enterprises have to suffer grievous loss due to the theft of intellectual property right. Before now, only the civil remedies can be requested under the Contract Law, Restatement of Unfair Competition, Restatement of Torts or Uniform Trade Secret Act, and no special civil penalty was prescribed. But under EEA Section 1831, any organization that commits any offence shall be fined not more than $10,000,000. The penalty can prevent the improper disclosure of trade secrets and protect the national economic interests.

Previously, trade secrets were misappropriated, and no effective laws prohibit economic espionage, so the rights and interests of the USA enterprises cannot be protected if encountering foreign economic espionage. The proposed H.R.2435 Bill, i.e. Cyber Security Information Act in July 10, 2001. The purpose of this Act is to encourage the secure disclosure and protect exchange of information about cyber security problems, solutions, test practices and test results, and related matters in connection with critical infrastructure protection. Many information technology computer systems, software programs, and similar facilities are essential to the functioning of markets, commerce, consumer products, utilities, government, and safety and defense systems, in the United States and throughout the world. Protecting systems and products against domestic and international attacks or misuse through the Internet, public, or private telecommunications systems, or similar means is a matter of national and global interest; greatly enhance the ability of private and public entities to improve their cyber security. The purposes of this Act are to promote the secure disclosure and protected exchange of cyber security information, to assist private industry and government in responding effectively and rapidly to cyber security problems, to lessen burdens on interstate commerce by establishing certain legal principles in connection with the secure disclosure and protected exchange of cyber security information and to protect the legitimate users of cyber networks and systems, and to protect the privacy and confidentiality of shared information. Szu-Ting Chen, member of congress proposed Cyber Security Information Act, for details see http://stlc.iii.org.tw/tlnews (search date: Aug. 12, 2007). As for the security of information, there is exemption to disclosure under Freedom of Information Act (FOIA)(U.S.C. Sec.552(a)), in principle the federal government shall provide the relevant data for the applicants except the trade secrets and financial information. The Cyber Security Information related to the ability of any protected system, or critical infrastructure to resist intentional interference, compromise, or incapacitation through the misuse of or unauthorized access to or, that harms interstate commerce of the United States. Under this Act, the protection is accomplished through government, private industry and private sectors. In fact, United States appeals to various critical infrastructures, the federal agencies and private sectors have established Information Sharing and Analysis Centers (ISACs) for cooperation in information security. Szu-Ting Chen, Id. Due to computer hacking and internet application, the speed and channel of disclosure of trade secrets are difficult to control. This act can promote security of information, encourage the secure disclosure and protect exchange of information.

Legislators find the main point is to protect the value of intellectual property and not to provide the open or creative environment during enactment of EEA, and the legislators cannot consider the direction of invention and innovation. The protection of intellectual property is to prevent the disclosure of trade secrets. The enactment of laws provide the better blueprint for the future research. Rochelle Cooper Dreyfuss, How Well Should We Be Allowed To Hide
disclosure of trade secrets threatens the formation of the intelligent assets and enterprises. The FBI and Chamber of Commerce of the United States of America formulated the measures to crack down economic espionage, and meanwhile they cooperate with information center and overseas chambers of commerce to crack down the theft of intellectual property.

III. Risks to trade secret protection posed by computerization

The ubiquitous use of computer and internet results in the new risks to trade secrets protection. The possibility of disclosure or theft of the commercial secrets is higher than before, and enterprises have to face more risks and suffer more loss of business profits. The request of employee’s duty of secrecy and no-compete limitation restrain the future development of former employees. In the following section, we discuss how to reasonably protect trade secrets in the society where information and computer are prevailing.

1. Internet increases the channels for disclosure of secret information

The internet development makes information disseminate without limitation. The informationization changes the contents (especially the amount) and speed of the information dissemination. Lots of information (data, report or form, program and formula) can be disclosed in extremely short time. Nowadays, employees can easily access the core information of a corporation, which is helpful to business operation, production or design and invention of new products. However this may also cause an enterprise to lose its own trade secrets. An enterprise must weigh the pros and cons.

During the use of internet, enterprises should educate their employees to pay attention to: 1) unintentional disclose the confidential secrets during free time because some competitors may set trap; 2) email transmission, the mail contents can be read and backed up through server, the email password can be cracked; 3) wireless network has more risks than wire network, the third person can intercept signals and communication on wireless network, and this interception is more convenient than the wire internet.

(1) Whether the acquisition of information from internet is improper

The wrongful disclosure of trade secrets spreads widely on internet and become common. Any employee or principal acquires by improper means a trade secret through his duties or work, but the parties are restricted by employment and fiduciary duty. The most widely quoted definition of a “trade secret” prior to the Uniform Trade Secret Act (UTSA) was that of the Restatement of Torts, and fiduciary duties are owed by persons who have been placed in positions that require loyalty and the utmost good faith to a

---

81 Id. at 268-269.
82 Id at 270.
83 See Restatement (First) of Torts § 757 cmt. a (1939), see the preceding paragraph.
principal or principals. In addition, a trade secret may be known through employment, appointment, and contract or business. The use of internet changes the channel of trade secrets. The acquisition of information via internet should be protected by the First Constitutional Amendment to ensure freedom of information. Weil, Gotshal & Manges, representing DVD Copy Control Association, filed a complaint in Superior Court of California, County of Santa Clara requesting a temporary restraining order. The request was denied. The protection of trade secrets has no conflict with freedom of information. Therefore, the information on internet can be accessed lawfully.

If there is no employment relationship or fiduciary and secrecy duty between person who knew secrets and the holder of a secret, the parties should be protected by First Amendment to ensure freedom of information. For example, in the case of Motor Co. v. Lane, the Defendant, engaging in website related to the information of Ford motors and other products, one day he acquired the confidential information provided by anonymous source and promised not to disclose it, and however the Defendant posted some of the confidential information on his website. It is judged that information is about the nature of the Ford motors, and the public has the right to know. The Court identifies the Defendant action impacts the interest of Ford, but the First Amendment shall prevail. Thus, Plaintiffs motion for a preliminary injunction enjoining Defendant is denied.

(2) Information is not confidential if it is sold on internet

In computer companies, the hardware structures, source codes of software are the trade secrets during the research, launching and sales of products. If an employee sells such information on internet, no matter how short is the time, the information is not confidential. The request for relief does not approach a trade secrets misappropriation. In the information times, the above situation often occurs. Take Religious Technology Center v. Lerma as an example, the former employee posted the confidential documents of the Church of Scientology (hereafter referred to as the “Church”) on internet. The plaintiff (the Church) prosecutes the Defendant’s infringement of the trade secrets and The Washington Post publication of some of trade secrets.

Once the confidential information is disclosed, it is no longer trade secrets. In the Church case, the Court judges it is not a dispute about trade

85 Elisabeth A. Rowe, Saving Trade Secret Disclosures on the Internet Through Sequential Preservation, 42 Wake Forest L. Rev. 24 (spring 2007).
86 75 P.3d at 19.
87 Id. at 10 n.5.
88 Rowe, supra note .at 25.
90 Id. at 747.
91 The similar cases such as United States v. Genovese, 409 F. Supp. 2d 253 (S.D.N.Y. 2005)
93 Id. at 1365.
secrets. Even if the Plaintiff tries its best to keep confidential the information, the information is still disclosed, and thus the judgment is entered for the defendants; there is another similar case, Religious Tech. Ctr. v. Netcom On-Line Commc’n Servs. Inc., even under the Uniform Trade Secret Act, the Plaintiff meets the essential conditions of trade secrets protection, such as locking the confidential documents, setting recognition code, installation of electronic sensing device, supply of security guard, and signature of confidentiality contract, however the Defendant posted the documents on internet, the public can access the information, it is not necessary to order the injunction against the Defendant, and the Plaintiff cannot claim the information as a trade secret.

Six months after adjudication, the church organization conducted consumer surveys to prove the preceding documents have not been know by the public, but the Court dose not acknowledge the validity and relevance of the survey, because the participants are the general public not the church opponents. The public knowing does not pose a threat to the church, but if the trade secrets are known by the opponent, this may posses a great threat to the church. The Court reconsiders the judgment is not favorable to the victim and may protect the opponents who knew the confidential information. Therefore the Court orders injunction to enjoin the Defendant’s disclosing of the documents.

In the case of United States v. Genovese, the Defendant Genovese sold the program code of Microsoft, and was prosecuted for violation of Economic Espionage Act of 1996. The Defendant protested conviction violates the First Amendment guaranteeing free speech. The Court judged the First Amendment protects the people’ right to know and the freedom of the computer program but not the action for obtaining personal economic benefit. The Defendant thinks the Microsoft does not make every effort to protect its trade secrets and the program has not been known by the public.

Dose the information posted on the internet infringe the rights and interests of holder of trade secrets? In the following, we discuss whether the internet affects the essential elements of trade secrets. If affecting the essential elements, the disclosing of the information may infringe the rights of the holder of trade secrets. In addition, if secret information is known by a third person via internet, which causes damages to the holder of the secret information, may the holder request for liability? If the trade secrets of company A are posted by person B on internet, person C uses the information,
which causes damages to the company. There was a case in California in 2006; the secret information of some company was published on the newspaper or magazines by the journalist and the editor, who are responsible for infringement due to disclosure of trade secrets. As previously mentioned, the Uniform Trade Secrets Act defines the “improper means”, the company A can request the persons B and C to compensate its damages. However person B posted the secrets on interne (public domain), so any person can access them. Can company A request C to compensate its damages?

In the case of Religious Technology Center, the confidential information had posted on internet for ten days, whether the information is known by the public, the opinion of the Court is positive, the public can easily access to the internet. The information on internet is no longer secret, similarly, in another case the opinion of the judge is the same. Therefore, whether the public can easily access to the information, trade secrets are disclosed or acquired by improper means, the third person knows or has reason to know that the trade secret was acquired by improper means; if the trade secrets are acquired by search engine not hacking, the trade secret is not infringed, and meanwhile the freedom of information is protected by the First Amendment.

2. Increasing cost for training and security

The subject of the disclosure or theft of trade is a “person”. Thus, the moral awareness of employees should be enhanced, the standard of the occupational ethic should be raised, the education and training should be carried out from time to time. Efforts should be made to guide the attitude of the users of trade secrets. Accordingly, the work environment, remuneration and welfare of employees should be improved. Suggestions: 1. Either in the open meeting or speech, the enterprises should let the employees know the secrecy of information to establish the good faith between employers and employees, let the employees know the written information and requirement of corporation through firewall, message board and cooperate website or issuing internal magazines, newspapers and messages. 2. Establishment of relevant department to protect the intellectual property right and other rights and interests of corporation, and meanwhile appoint special person to supervise and manage these matters (profit, security setting, cooperation interests, and excessive costs should be considered). 3. Increase the

---

102 See O’Grady v. Superior Court, 44 Cal. Rptr, 3d 72, 98 (Ct. App. 2006).
104 In the previous judgment, the third person is not liable for the liability if not intentionally. See Lockridge v. Tweco Prods., Inc., 497 P. 2d 131, 134-35 (Kan. 1972) quoting Underwater Storage, Inc. v. U.S. Rubber Co., 371 F.2d 950, 955 (D.C.Cir.1966).
107 See DVD Copy Control Ass’n v. Bunner, 75 P. 3d 10 n.5 (Cal. 2003).
108 HP filed a complaint against Acer in a Texas court, which claimed that Acer was infringing patents covering technologies such as, covering technologies such as read/write optical drives, power management in notebooks and digital bus arrangement. As with that complaint, the new lawsuit filed on Thursday--seeks to stop Taiwan-based Acer from exporting its PCs to the U.S. and selling them there. The areas of focus of the four patents this time range from thermal
decompile systems or devices, although the cost increases, the effect is obvious; hire computer and information experts, establish the relevant law department to take charge of security or protection and inspection of information. 4. Enhance the security work; the subcontractor should keep confidential information of the corporation, prevent embezzlement, especially the former employee's infringement of data or database of the corporation, so the protection should be enhanced.

The patent law always protects the secrecy of the patents, and thus the exclusity of the patents is broader than that of trade secrets, provided that the patent is valid. If the patent is disclosed or stolen, the patent will fail to be approved. Take Lorenz v. Colgate-Palmolive-Peet Co for example\textsuperscript{109}, the Plaintiff claimed the Defendant’s perfumed soap patent is invalid, because it was told to Defendant by Plaintiff; the Defendant alleged he had known the formula before the Plaintiff applied for patent, namely, the previous disclosure make the patent invalid.

This Court thinks the information has been known and used by the public. In order to maintain the well-being of the people, the formula should be disclosed as early as possible. Therefore the Plaintiff lost a lawsuit. In another one, Evans Cooling Systems, Inc, v. General Motors Corp. in 1997\textsuperscript{110}, the Plaintiff prosecuted the Defendant GM for infringement of its engine cooling system, the Defendant claims that the patent is invalid, because GM had sold the motors with the engine cooling system before the Plaintiff applied for patent. The Plaintiff alleges the selling is unlawful due to theft of the patent design\textsuperscript{111}. The Court thinks that the Defendant dealer had not knew the content of the patent including the dispute of cooling system. Due to the engine has been used in public, in order to maintain the well-being of the people, and protect the user who does not know, the Court judged the Plaintiff lost the lawsuit. As for the Defendant's infringement of the trade secrets of the Plaintiff, the Plaintiff can provide further evidence\textsuperscript{112}.

management to video control, and are being disputed through a complaint filed with the same court and a separate complaint lodged with the U.S. International Trade Commission. “HP believes Acer has been importing into the United States and selling computer products that use HP's patented technologies without permission. HP will continue to take action to protect its intellectual property against unauthorized use.” a statement from HP said. Reported by Comprehensive Telecommunication, [HP sues Acer again over patent infringement], World Daily News Sec. E2, Apr. 23, 2007, when we read the daily newspapers and magazines, the cases involved in infringement of intellectual property rights, the large corporation can establish law department to file a lawsuit and seek relief.

\textsuperscript{109} 167 E2d 423 (3d Cir. 1948).
\textsuperscript{110} 125 F.3d 1448 (Fed. Cir. 1997).
\textsuperscript{111} Id. at 1450.
\textsuperscript{112} Id. at 1454. Part of fact is cited, and the analysis and conclusion are the opinion of the author.

Two cases are separated in time by many years, but overlap between patent law and trade secrets protection can be found in terms of their judgments. In Taiwan, the Article 16 of the Trade Secret Law is applied to this case. From 1996 till now, in Intellectual Property Office, “Research on Taiwan Trade Secrets Legal System”, Planner of Attorney Jing Chang proposed amendment, but it has not been implemented. Taiwan has the written laws. Under the laws, the patents are protected by the Patent Law. USA adopts precedents and makes laws according to the cases. The Anglo-American law system is suitable standard to resolve some
3. Importance of Business Strife Limitation Clause and Confidentiality Agreement

The informationization makes the former employees more easily acquire the secret information by password and other approaches and steps known during employment. Take the adjudication of the district court in Ohio, USA as an example, and the Defendant worked for a corporation which is the opponent of his former corporation after resignation, he knew the approach to the trade secrets. The Plaintiff requests the Defendant to perform the obligations of business strife limitation and the Court to issue the injunction against the Defendant to prevent the Defendant from disclosing trade secret. The District Court denies the injunction due to the Defendant has not caused the material damages to the Plaintiff.

After the Plaintiff filed the appeal, the appeals court vacates the opinion of the district court, and thinks it is not necessary to prove the Defendant causes actual-harm, as long as the following essential conditions are met, the threat-of-harm is caused: 1) claimant must be the party to be protected; 2) if the injunction is not approved, claimant will suffer the unrecoverable damages; 3) the issue of injunction will not cause the inequitable damages to the third person; 4) the issue of injunction helps to maintain the public interest. Based on the above-mentioned reasons, the appeals court thinks the district court denies the request for injunction is incorrect. By adopting the threat-of-harm standard, the request for injunction should be approved, because the Defendant knew many trade secrets of the Plaintiff.

On January 5, 2007, California Court of Appeal accepted the case of Aldrich Supply Company, Inc. v. Richard Hanks. The Plaintiff Aldrich Supply Company, Inc. (Aldrich) vends PVC pipes. The Defendant Hanks, resigned from Aldrich, is prosecuted for misappropriation of trade secrets of the Plaintiff. The California District Court judges the Plaintiff lost the lawsuit. The Plaintiff refuses to accept the decision and file an appeal. The District Court denies the Defendant’s requests for returning attorney fee. The Defendant file an appeal for this request, the Court of Appeal affirms the original judgment.

The Plaintiff’s company was founded in 1947. The Defendant was employed by the Plaintiff in 1977, and took charge of the business affair. The Defendant did this kind of job since 1966, and was promoted to the vice manager in 1987. Both parties signed five years employment contract, in which the Defendant shall not disclose any trade secret of the Plaintiff for two years after resignation, and the Defendant shall not employ any employees of the Plaintiff or make the employees resign. In 1998, the Defendant was

---

issues about the litigation involved in technical fields, for the Taiwan Trade Secrets Legal System, see Chang, C., Construction and Validity of Taiwan Trade Secret Law, pp.1-2, Sharing Publishing, Apr. 2007.


promoted to the general manager. Till 2001, the Daly reduced 5% of salaries of Hanks due to poor performance of Defendant’s son (also worked for Aldrich) and suspected the Defendant’s loyalty, so the Defendant was angry to tender his resignation on November 30 in the same year. Afterwards, the Defendant founded the American Pipe with the help of friends, became the rival of the Plaintiff. After two months, the Plaintiff prosecuted the Defendant for improper use of trade secrets of the Plaintiff and unfair competition, which destroys the profits and affects the anticipated economic benefit of the Plaintiff.

Hanks protested that Plaintiff had not identified the so-called trade secrets and had not taken any special measures to protect them; secondly, the Defendant had not used any secret information of the Plaintiff in the new company American Pipe. The Plaintiff Aldrich protested that the Defendant used the client lists and the relevant information, which are the trade secret of the Plaintiff. The judgment was entered in favor of the Defendant, but Defendant requests the Plaintiff to pay for attorney fee is rejected.

In the case of Certainteed Corporation v. Jerome O. Williams\textsuperscript{116}, the Plaintiff (employer) prosecuted the employees for violation of the Business Strife Limitation, the U.S. Court of Appeals (7 Cir) supported the Defendant at the first trial, so the Plaintiff filed an appeal. In accordance with the Pennsylvania laws, the court of appeal thinks the Plaintiff has no need to prove the former employee uses the confidential information in his new work; if the former employee may use the information, the employer may request for injunction; when the Defendant worked for the Plaintiff between 2002 and 2006, he had signed the business strife limitation clause in 2002. The Defendant shall not work for the opponent of his former corporation in one year after resignation without the prior consent of the Plaintiff; the Defendant protested that headquarter of the CertainTeed locates in Pennsylvania, and the business strife limitation clause is invalid according to the Pennsylvania laws.

In addition to the employees, the manufacturers who cooperate with the corporation and any person who may know the trade secrets of the corporation should sign the confidentiality contract so as to avoid the unintentional disclosure of secret information during the introduction of products and process. Nowadays, enterprise alliance, mergers and acquisitions are often implemented. In the information society, the enterprise can receive the data of others in very short time. If the cooperation is not successful, or the person disclose the known information, the cooperation result, and the stock price of the corporation, even the trust relations between the investor and shareholder will be affected. Therefore, this situation may cause the disclosure of secret information\textsuperscript{117}.


\textsuperscript{117} In 2004, Samsung and Sony invested $2 billion USD to establish a new corporation for development of 7 G LCD line. Although Samsung compete with Sony on TV market, outsiders are concerned about Samsung will learn the technology from Sony, and reversely hit Sony. The fact proves the Sony’s decision is right. Kuang, W.C., “Clasp Core Technology to Cooperate with Foes in other Fields”. Business Weekly, Issue 906, p.53, Apr. 17, 2006. The
The attorneys advise enterprises that prior protection is better than ex post dispute. When an enterprise grants exclusive license (or right of agency) or non-exclusive license or shifts investment (sole ownership or joint ownership) and implements merger & acquisition, it should protect its intellectual property right, firstly register its trademarks and patents and then seek the protection of copyright and trade secrets; the types of cooperation are sole ownership, joint ownership, exclusive license and non-exclusive license\(^\text{118}\), and thus the standards for protection of intellectual property rights are different. This paper considers the partner or the authorized licensee should meet the requirement of the license and also sign the confidentiality contract to prevent the disclosing the secret information during cooperation or authorization or after the termination of them.

**4. Summary**

The market information is ever changing. Mergers and acquisitions\(^\text{119}\), job-hopping and undermining become more and more popular\(^\text{120}\). As high-tech tools and internet are developing fast, the types of the transaction and marketplace (E-commerce) changes quickly. In the information transmission and personnel adjustment (both buyer and seller have never meet each other, even in the employment relationship, both parties may contact with each other via internet), the protection of trade secret is based on the mutual trust. If the duty of fidelity and good faith is breached, pursue the economic benefit and severe statutes or enforcement may cause some persons to crack passwords and seek the approach to theft. In the next, we discuss whether the USA laws can provide the reference for Taiwan to legislate or amend the statutes to consider, doubts and good-faith basis may affect the relations between parities, which may result in profits or losses.

\(^{118}\) See David H. Kennedy, Selected Intellectual Property Issues Arising in the Context of Acquisitions, 893, PLI/PAT 158-160, (March-May, 2007). The author is the senior practicing lawyer, specializing in commercial regulations and intellectual property right laws.

\(^{119}\) Take ASUS Computer as an example, in 2005, ASUS allied with Advantech to establish Advansus and enter into industrial computer market with high gross profits. In March, ASUS acquire telecommunication maker Askey to expand the market sharing, become the second-largest telecommunication maker. The acquisition make ASUS enter into new market quickly, and enjoy the price negotiation chance. Chen, M.J., “ASUS Computer, consolidated income increase 43%, high growth by basic skill cultivation”, Commonwealth, Issue 345, p.234, May 3, 2006.

\(^{120}\) In 2005, Kai-fu Li left Microsoft to take a position at Google. In doing so, Lee allegedly violated a non-compete agreement. Many Chinese people think Kai-fu Li violated the important ethical rule--honesty which is often emphasized by him. Microsoft thinks he should not work for the company specified in the non-compete agreement. Kai-fu Li thinks “no employer has the right to request an employee to work for himself for ever, this is misunderstood by the Chinese people, Kai-fu Li signed the no-compete clause for Microsoft, a non-compete clause is a term that one party (usually an employee) agrees to not pursue a similar profession or trade in competition against anther party (usually the employer ); this is not consistent with USA laws, under the Washington law, the contract is not allowed me to do the similar job of the competitor. He thinks the job is different from the job that he did for Microsoft”. Chang, Y.J., Chang, W.T., “four Kai-fu Li Google convulsion”, Business Weekly, Issue 906, pp.36, 40, Apr. 17, 2006, under the different background, the interpretation of honesty is different. At last, the Court judges that Kai-fu Li moving from Microsoft to Google does not violate the laws, ibid.
IV. Suggestions for trade secrets protection posed by computerization in Taiwan (Conclusion)

In USA, the head offices control the confidential information, such as financial statement, and R&D information. The production is shifted to the Mexico and Chinese Mainland\(^\text{121}\) where the labor cost is cheap. Thus both the protection of confidential information and pursuit of profit are ensured. In the following part, we discuss the business strategies and protection of intellectual property right, and make suggestions.

1. Operation Strategies\(^\text{122}\)

(1) Fortress monopoly

The trade secrets can be protected through fortress monopoly, such as application for patents. For instance, large pharmaceutical factories (such as Merck and Pfizer) devote a large amount of manpower, materials and capital in R&D. The invention and production of a new drug require very long time. After the expiration of the patent right, the factories should enhance internal organization and management, reduce the cost and compete with other opponents. The disadvantages of the fortress monopoly is the factories have to file a lawsuit at any time to prevent fraudulent use and imitation by others, and the fortress monopoly may be lost due to unfair competition\(^\text{123}\).

(2) Value-added monopoly

In addition to the essential products, enterprises should devote to the development of additional products to add the value. For example, GM (General Motors) launched On-Star\(^\text{124}\), which makes the motor functions different from the other brands and increases market sales and competitive power. Thus, the products have more selling points and stunts in the sales promotion. After expiration of the patent right during the preceding monopoly, the ingredients and formula of the drugs can be protected as trade secrets; as for the value-added monopoly, the functions of the additional products and the additional protects are the trade secrets. However, the prior protection of information should be carried out to prevent the disclosure impacting the business chances\(^\text{125}\).

(3) Hub monopoly

A corporation usually has core products based on its main technology, and authorizes the technology to others. The others can use this technology due to the legal authorization, and the products can be carried forward. For example, Philips and Sony developed CD technology, and the videocorder was invented based on the technology. The computer can use CD so as to save a great


\(^{122}\) See above. Id. at p2-p3.

\(^{123}\) Id.

\(^{124}\) On Star is a optional service system for GM vehicles, and it relies on CDMA mobile phone voice and data communication as well location information using GPS technology. Log in: http://www.onstar.com/us_english/jsp/plans/index.jsp (Search date: Aug. 12, 2007).

\(^{125}\) Id.
amount of space and devices.

(4) Monopoly-in-a-box

This is similar with the section 3, but the difference is that the monopoly-in-a-box grants the exclusive license of products to another corporation. The advantage is that the resources such as marketing, public relations, and business strategy can be utilized by other corporation, and the products can be promoted by other corporation. For example, some smaller biochemical companies hope to cooperate with large pharmaceutical factories to promote their products, increase the sales and enhance effect of advertising because the large pharmaceutical factories have good reputation. However the exclusive license should specify the protection of trade secrets, otherwise, the raw materials and process of the products may be disclosed during the production.

In the preceding paragraphs, the advantages and disadvantages of business strategies adopted for the protection of the intellectual property rights especially trade secrets are discussed. The advantages of the operation strategies (1), (3) and (4) are cheap labor cost and cooperation with large manufacturers, more capitals invested in R&D, so the protection of the intellectual property right can be enhanced, and the profit and development can be balanced; the disadvantage is that the possibility of the theft of trade secrets increases, and thus the cost for lawsuit and relief increases and the operation efficiency is affected.

If adopting the strategy (2) value-added monopoly, the outcome of the products globalization is to attach importance to the economic benefit and neglect the protection of intellectual property right. In order to maintain long-term operation and client relations, the products should be innovated, and meanwhile the trained professional persons, organizations or individuals should pay attention to the confidentiality of documents and data. The outcome of computerization including the use of e-mail, voice mail message, text short message and other modern communication tools, causes the change of information delete, identification and storage, and the standard for protection of secrets should be upgraded.

2. Intellectual Property Rights

No matter what operation strategies an enterprise adopts, the obtainment, assignation and contents of the intellectual property rights should be carried out in accordance with written contract and determined procedure.

(1) Written Contract

1. confirm the type of contract, such as employment, work (full-time or part-
time), shift in investment, co-research, acquisition of intellectual property.
2. technical fields, labor power, capital ratio and scope of trade secrets.
3. the personnel providing the financial information and the lawsuit, or the external inspectors or experts from the R&D department or laboratory should sign the confidentiality or undisclosed contract.
4. pay attention to affiliated enterprises or cooperative manufacturers, remind the employees that the use of third-person technology as well as the quoted data from the academic or research institutions in industry-academy cooperation requires authorization or indication of the source of information.
5. clearly state the documents or database software, including free software or the software downloaded from internet.
6. the letter of authorization for the registered patent and trademark should be obtained (after expiration of authorization, the trade secret protection can be claimed).
7. affirm whether products use the raw materials of the third person, and indicates them if any.

The parties may think the above procedures are complex. However, according to a survey of 1478 manufacturers, 24 industries (surveyed industries totals to 33) think the confidentiality of R&D information is the most important element. In addition to the written contact, next we discuss other confirmation procedures to ensure the integrity of trade secrets.

3. Confirmation procedure
1. apply for registration of intellectual property right, ensure the proprietary right and exclusive right during the term of protection, and handle the registration procedure.
2. file a lawsuit if have the disputed intellectual property, determine the amount of the damages and contents.
3. confirm the contents and effect of the intellectual property, especially the estimated effect on the market.
4. plan and implement the management of intellectual property rights, the supervision is carried out by special persons and departments, appoint the law firms or consultation corporation to take charge of these matters.
5. confirm the confidential information related to the unregistered trademark and patent, or the computer software; the famous formula of Coca Cola is still the trade secret, the protection of trade secrets can cover the intellectual property and other rights, as long as the they meet the essential conditions of trade secrets.
6. the software data should be encrypted or protected through various technologies, the products are equipped with tamper-evident device or some

---

131 See Melvin C. Garner, Creating and Managing IP that is Tailored to Your business Objectives, 893 PLI/Pat 33-34, (March-May, 2007).
protection measures are taken\textsuperscript{133}.  

7. during the technical and economic cooperation with other parties, provide the semi-finished products manufactured by using the key technology, for example, the Coca Cola only provides the concentrate and non-core technology for the licensed Coca-Cola bottlers throughout the world, the ingredients and formula is not disclosed\textsuperscript{134}.

4. Summary

A desktop or a laptop may exist many risks to disclose the trade secrets\textsuperscript{135}. Firstly, large enterprises subcontract the cleaning work to external cleaning companies. When cleaners enter the vacant office, the employees should take measures to protect or encrypt their information on the desk or computer. Suggestions: 1) update and check the passwords, the holder shall not name or birthday as passwords, the passwords should change every month (or two and three months); 2) the laptop is easily stolen or lost, and thus the important information should not be stored in the laptop for long time, after use, the data should be backed up and deleted from the laptop\textsuperscript{136}; 3) when the outdated computers or other relevant equipment (hardware) is unwanted, the data should be deleted or backed up, it is recommended that the data in the hardware should be firstly deleted before discard, and careful inspection is required\textsuperscript{137}.

The widespread use of computers and advent of information society result in many new problems and raise doubts about intellectual property protection. Some problems can be solved pursuant to Taiwan laws, by reference to USA legislation and experience and improvement of written codes. However the technical tools and technologies are changing quickly, we will face more and more problems. We should understand the importance of trade secrets protection and clear know the definition and scope of trade secrets. It is better to carry out the prior protection (such as signature of written contracts) than the relief (lawsuit or compensation). The explicit written contracts shall be combined with staff training and business strife limitation clause. Enterprises should provide the better work environment, remuneration and advanced study for their employees to reduce the personnel transfer. Thus the integrity of trade secrets, stable profits, win-win for labor and capitals can be ensured and the he business operation information society will be improved further.


\textsuperscript{134} See the example in 133, Chinese Mainland First Military Medial University provides the semi-finished toothpaste for a tube factor to process the finished products.


\textsuperscript{136} Id. at 265-267.

\textsuperscript{137} Id. at 270.
References
Chinese
1. Publications

2. Articles
   2. Lin, H.L., Research and Discussion of USA Economic Espionage Act— including strategies for Taiwanese Employees, master’s thesis, Graduate Institute of Law, Tung Hai University, June 2000.

3. Electronic articles
   3. Chen, S.T., “Member of Congress Propose the Cyber Security


English

I. Articles


13. Robert Unikel, Bridging the “Trade Secret” Gap: Protecting “Confidential Information” Not Rising to the Level of Trade Secrets, 29
II. Cases


5. DVD Copy Control Ass’n v. Banne, 75 P.3d at 19.


III. Electronic Articles


2. David B. Fein and Mark W. Heaphy, Companies Have Options When Systems Hacked Same technologies that empower corporations can expose vital proprietary information, 27 Conn. L. Trib. 5 (Oct. 15, 2001).


4. Fred katayama, Hacker hits up to 8M credit cards, Secret Service and FBI probe security breach of Visa, MasterCard, Amex and Discover card accounts, CNN MONEY,


