Trade secrets rules, regulation and enforcement in China and the U.S. — a comparative analysis

By Jeffrey J. Zuber

Over the last two decades, China has developed a comprehensive set of laws and regulations designed to protect and enforce company trade secrets. In many ways, Chinese trade secret laws offer more protection for the owners of trade secrets than U.S. trade secret laws. However, enforcement is difficult, as there is a high burden of proof on plaintiffs, and as courts have struggled to keep up with changing laws and have been slow to enforce new intellectual property rights.

"Trade secrets" are defined similarly in both China and the U.S., and both countries require an owner of those secrets to take certain preventative measures before he can claim trade secret protection and enforce against infringement.

This article will compare the rules, regulations, and enforcement provisions of both Chinese and U.S. trade secret law. It will also discuss protective measures that trade secret owners can take to prevent infringement and enforce their right under the laws of both countries.

Defining a "trade secret"

As in most countries that have adopted trade secret laws, the elements of a trade secret in China and the U.S. focus on the secrecy of the information, the economic value of the information, and the efforts that the trade secret owner has taken to keep the information confidential.

1. China

China has a number of laws that address trade secrets, but the primary law on the topic is China's *Anti-Unfair Competition Law* (AUCL), which came into force on December 1, 1993. Article 10 of the AUCL defines a trade secret as follows: "technical and operational information which is not known to the public, which is capable of bringing economic benefits to the owner of rights, which has practical applicability and which the owner of rights has taken measures to keep secret."[1]

In order to enforce a trade secret against infringement, all four elements of the Article 10 definition must be met. Chinese courts and scholars have interpreted each element as follows:

1) "Not known to the public:" The "public" in this definition does not refer to the general public, but to current or prospective industry competitors or people who want to obtain economic benefit by exploiting the secret. The "public" is also limited to the Chinese "public" – if a trade secret is known outside of China but not inside China, it is considered "unknown to the public" under this definition. "Unknown" means secret and not accessible through public channels.[2]

2) "Potential economic benefits:" Through tangible or intangible means, the trade secret must be able to generate profit or commercial value, or provide a competitive advantage.

3) "Practical applicability:" The information should be specific and immediately useful and applicable to industrial and business applications. It cannot be mere theory or a general principle.

4) "Measures to keep secret:" Before an owner of a trade secret can claim infringement, he must show that he took proper and reasonable steps to keep the information secret, and he should be able to trace those steps through written records. For a list of the types of measures that can be taken, see below.

2. United States

The United States has one uniform statutory provision, adopted by the individual states, that addresses private civil remedies for trade secret infringement, and a separate federal statute that makes some trade secret misappropriation a federal crime.

The majority of states in the U.S. and the District of Columbia have adopted and codified the *Uniform Trade Secrets Act* (USTA). The USTA's definition of a trade secret includes those considerations of secrecy, value and security measures:

Information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[3]

The USTA does enable claims of third party liability against someone who did not directly take the trade secret, but who received it from the person who took the trade secret.

In contrast to Chinese law, in the U.S., information does not need to have immediate practical applicability to be considered a trade secret. A plaintiff might be able to prove that a business plan or corporate strategy is a protectable trade secret in the U.S..

The U.S. *Economic Espionage Act* of 1996 (EEA), 18 USC §1831 *et seq.*, which makes theft or misappropriation of trade secrets a federal crime, includes a slightly broader definition of a trade secret than the USTA. It refers to trade secrets as being "tangible or intangible," and it also states that something might be a trade secret regardless of how it is stored. 18 USC §1839(3). Under the EEA, then, a trade secret might be an idea or process that is wholly "stored" in an employee's memory.

Infringing on a trade secret

1. China

Notably, China has legal provisions that clearly recognize third-party liability for trade secret infringement. Article 10 of the AUCL defines the following acts as trade secret infringement:

1) Obtaining trade secrets from the owner by stealing, promising gain, using coercion or other improper means;

2) Disclosing, using or allowing others to use trade secrets obtained by stealing, promising gain, using coercion or other improper means;

3) Disclosing, using or allowing others to use trade secrets that a party has obtained by breaking an agreement or disregarding the requirements of the trade secret owner to maintain the trade secret in confidence;

4) Where a third party obtains, uses or discloses someone else's trade secret when he had, or should have had, awareness of the illegal acts mentioned above.

2. United States

Civil actions

In the U.S., a claim of trade secret infringement is called "Misappropriation of a Trade Secret." Under the USTA, misappropriation means:

1) The obtaining of a trade secret by a person who knows or has reason to know that the trade secret was acquired by improper means such as theft, bribery, misrepresentation, breach or inducement of a breach of a duty of secrecy, and espionage; or

2) The disclosure or use of a trade secret by a person who improperly obtained the trade secret or who, at the time of disclosure or use, knew or had reason to know that the trade secret was:

a. obtained through improper means; or

b. acquired under circumstances in which there was a duty to maintain its secrecy or to limit its use; or

c. obtained from a person who had a duty to maintain its secrecy or to limit its use.

d. in fact a trade secret that had been obtained by accident or mistake.[4]

The USTA specifically states that reverse engineering and independent derivation do not constitute misappropriation.[5] The USTA does enable claims of third party liability against someone who did not directly take the trade secret, but who received it from the person who took the trade secret. The third party can only be held liable if he or she knew or should have known, based on the surrounding circumstances, that the information was a trade secret that had been wrongfully obtained and disclosed.

Criminal actions

The EEA defines the following as federal crimes:

Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly

1) steals or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

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

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

4) attempts to commit any offense described in any of

paragraphs (1) through (3); or

5) conspires with one or more other persons to commit any offense described in any paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy shall be liable for the recited penalties.[6]

Enforcement and liability for infringement

1. China

Enforcement of trade secrets can be difficult in China because there is a high burden of proof on the plaintiff. However, an owner of a trade secret has several options available in China in the event of infringement, if he can successfully prove that the information was indeed a trade secret:

1) Administrative Action: Under Article 15 of the *Unfair Competition Law,* when someone infringes on another's trade secrets, the trade secret owner can request enforcement by the Administration for Industry and Commerce (AIC). The AIC can order the infringing party to stop the infringing acts, order the return of stolen materials and information, order the destruction of any goods made with the trade secret, confiscate the infringer's illegal income, revoke the infringer's operating business license, and, in some circumstances, impose a fine of RMB10,000 to RMB200,000.[7] The AIC does not have the ability to award compensation to an aggrieved owner of a trade secret. AIC actions are most likely to be undertaken and succeed in clear cases of infringement, and even then, most pundits agree that the administrative fines are not big enough to act as a deterrent.

2) Lawsuit Claiming Civil Damages: A trade secret owner can file a lawsuit against an alleged infringer for damages. However, it's widely said that it's difficult for plaintiffs to prevail to any significant degree in trade secret infringement actions in China. While judges do tend to be fair, they are not obligated to follow precedent.

Monetary Damages: If damages to the trade secret owner are difficult to calculate, the court may instead base its damages calculation on the profits realized by the infringing party resulting from the infringement. A party found liable for infringement is also liable to pay the reasonable costs that the trade secret owner incurrent in investigating the case. It takes 4-7 years for a lawsuit to be heard, and significant damages awards are extremely rare.

Injunction: Injunctions are the most feasible and helpful remedy for a trade secret owner looking to stop infringement. A plaintiff can obtain a preliminary injunction if he can prove that: the information is a trade secret, the defendant's acts are causing irreparable harm, and the plaintiff is likely to prevail on the merits of the case. The plaintiff must also post a bond.

3) Criminal Penalty: Article 219 of the China's *Criminal Law* cites to the first three acts defined as infringement in the *Unfair Competition Law*, and states that anyone who commits one of those acts in a manner that causes "serious damage" to the trade secrets owner (over RMB 500,000 damage to an individual and more than RMB 1,500,000 to an enterprise), is liable for up to three years in jail and a fine.[8] There is an aggravation factor as well -- when the infringement causes "exceptionally serious" damage to the trade secret owner (RMB 2,500,000 for individuals and RMB 7,500,000 for enterprises), the infringer faces up to seven years in jail plus a fine. Many trade secret owners are hesitant to report bad acts to the police, however, because there is a risk of further exposure of the trade secret to public knowledge during the criminal prosecution.

2. United States

1) Private Litigation: The primary method of enforcement of trade secret rights in the U.S. is private litigation – an owner of a trade secret must file a lawsuit against those who misappropriated the trade secret. The USTA, which provides that trade secret litigation may proceed under seal to protect the trade secret, allows for a private plaintiff to pursue the following remedies:

a. Injunction: Actual or threatened misappropriation can be stopped through an injunction. The injunction can last as long as the trade secret is still a secret, and the court can continue the injunction even longer in order to eliminate any commercial advantage resulting from misappropriation. If the court determines that an injunction is not reasonable, it might condition the infringer's future use upon payment of a reasonable royalty to the trade secrets owner instead.[9]

Many trade secret owners are hesitant to report bad acts to the police, however, because there is a risk of further exposure of the trade secret to public knowledge during the criminal prosecution.

b. Compensatory Damages: Generally, a trade secret owner can recover for actual damages and unjust enrichment of the defendant resulting from the misappropriation. If those damages are not provable, the court may order the defendant to pay plaintiff a reasonable royalty for use of the trade secret instead.[10]

c. Exemplary Damages: If the plaintiff proves that the misappropriation was willful or malicious, the court may award exemplary damages in an amount not higher than twice the compensatory damages.[11]

d. Attorney's Fees: The Court may award attorneys fees to the prevailing party in a USTA-based action if the claim of misappropriation was made in bad faith, a motion to terminate an injunction is made or resisted in bad faith, or willful or malicious misappropriation exists.[12]

2) The *Economic Espionage Act*: Under the EEA, the U.S. Department of Justice can initiate criminal cases against those who misappropriate trade secrets related to products produced for or placed in interstate or foreign commerce. The burden on the government is high – it must prove, beyond a

reasonable doubt, that the accused infringer acted "deliberately and knowingly" at the time of the crime, and that the owner of the trade secret had taken reasonable measures to keep the valuable information secret. Largely because the threshold requirements are so high, only the most conspicuous and indefensible trade secret misappropriations get prosecuted under the EEA – there have been less than three dozen reported cases of the Department prosecuting under this act since it was implemented.

Conviction of theft of trade secrets under the EEA can result in a fine of up to $500,000 for an individual ($5 million for organizations), and/or imprisonment of up to ten years.[13] If the crime was committed to benefit any foreign government, instrumentality, or agent, the penalties increase to fines of up to $500,000 for an individual (up to $10 million for an organization), and/or imprisonment of up to 15 years.[14] Sentencing will also include criminal forfeiture of any property used to commit the violation and any property or proceeds derived or obtained as the result of the violation.[15]

Under Chinese law, there is no fixed term during which an employee must keep the trade secret confidential.

Under the EEA, the Attorney General may also seek to enjoin the infringer in a civil action.[16] However, the EEA does not provide for any compensation to the injured trade secrets owner.

Preventative measures

Enforcement of trade secret rights after infringement has occurred is difficult and expensive in both countries, though it is more difficult in China than the U.S. Therefore, it's critical that companies in China take comprehensive measures to protect their trade secrets and minimize the risk of infringement. Examples of security best practices that help protect trade secrets in any country include:

1) Trade Secret Audit: If development and protection of trade secrets is a dynamic process in your company, it's advisable to implement a regular method by which you screen your trade secret program, identify all potential trade secret information and ensure its current protection;

2) Restricted access areas, passwords and clearance levels for all users of the secret information;

3) Encrypting and physically securing of sensitive materials;

4) Enabling users of secret information to gain access to only the necessary part of the information, whenever possible;

5) Classification methods, including something as simple as the use of stamps on materials identifying them as "SECRET," "CONFIDENTIAL," etc;

6) Written confidentiality and non-compete agreements with everyone who will have any contact with trade secrets

7) Employee identification IDs and visitor clearance requirements;

8) Employee handbooks with provisions regarding trade secrets, photocopying policies, etc;

9) Reference and background checks on all managers, key employees and persons who will have regular access to any secret information;

10) Performing exit interviews with departing employees and providing a reminder of their continuing confidentiality obligations.

Both China and the U.S. have adopted a few specific legal provisions and applications regarding contracts that address trade secret issues:

1. China

1) Employee Confidentiality Agreements: Article 102 of the *Labour Law* provides that when an employee breaches "a confidentiality agreement provided in the employment contract, causing economic damages to the employer, he or she is responsible for compensating the damages according to the law."

Under Chinese law, there is no fixed term during which an employee must keep the trade secret confidential. The prevailing law states that both current and former employees must honor their obligation to keep the trade secret confidential for as long as the trade secret remains unknown to the public. Only if the trade secret becomes publicly available is the obligation of confidentiality lifted.[17]

Whenever possible, the confidentiality agreements should specifically identify the information that the employer wants to keep confidential – i.e. "all information regarding the specifications, development, and marketing (etc.) of Product X." The clearer it is that an employee was specifically instructed as to the confidential nature of information and agreed to keep it confidential, the stronger the case if an infringement action later becomes necessary. These agreements can be obtained from all employees of the trade secret owner, and from employees of any business partner that will have access to the trade secret.

2) Non-compete Agreements: Chinese law does not explicitly address non-compete agreements. Generally, Chinese courts have recognized and upheld non-compete agreements, so long as they contain the following provisions:

a. Specific scope of the non-compete limitation.

b. Term – must be fair and reasonable. Local regulations dictate a maximum length, typically a maximum of three years.

c. The Amount of Compensation – a non-compete is invalid in China unless the employer provides necessary economic compensation to the employee who is obligated not to compete during the non-compete period. Regulations provide that the minimum annual compensation for non-compete obligations is half of the employee's annual total income they received the year before he or she left.[18]

d. Method of payment of the compensation.

e. Liabilities for breach of the agreement.

As with confidentiality agreements, non-compete agreements

should endeavor to be as specific as possible in identifying exactly what secret information is covered by the non-compete.

2. United States

1) Nondisclosure/ Confidentiality Agreements: A nondisclosure agreement (NDA) creates a confidential relationship between a person who has a trade secret and the person to whom that secret is disclosed, whether employees or not.

A typical NDA includes the definition or scope of the confidential information, usually in the form of a list of types or categories of the information covered under the agreement. Many agreements also require that the receiving party keep the information secret for a limited period of years. Five years is a common length in American NDAs, but it's negotiable between the parties.

2) Covenants Not to Compete: A non-compete prohibits an employee from competing in the same business or industry with his former employer or prohibits an employee from servicing the same clients within that industry. The restriction is usually for a specified period of time within a limited geographic area, and the norms vary from jurisdiction to jurisdiction. Courts don't favor contracts that restrain free trade, so they tend to scrutinize non-competes fairly closely to ensure that the agreement only reaches as far as necessary to protect legitimate employer interests, not merely to prevent fair competition. Non-compete agreements are completely prohibited and unenforceable in California. Unlike similar agreements in China, they do not require an employer to compensate the employee during the non-compete term. IP

The restriction is usually for a specified period of time within a limited geographic area, and the norms vary from jurisdiction to jurisdiction.

Endnotes:

1.The Interpretation on the Application during the Trial of Civil Cases on Unfair Competition, promulgated by the Supreme People's Court of PRC, effective Feb. 1, 2007, lists the following circumstances that should be excluded from the scope of "business secrets:" general knowledge or known practices for those working in the technical or economic lines; information relating only to the product's size, structure, material, parts, etc. that the public could easily ascertain by looking at it after it enters the market; information that has been disclosed in publications or other media, or demonstrated in public reports or exhibitions; information that can be obtained by other public channels; information that can easily be obtained without paying certain prices.

2.This premise was set forth by Judge Cheng Yongshun in his book, *A Further Study of Trade Secret's Legal Features.*

3. National Conference of Commissioners on Uniform State Laws (1979) (amended 1985) at §1(4).

4. *Id.* at §1(2).

5. *Id.* at §1 Comment.

6.18 USC §1831(a) and 18 USC §1832(a).

7. Article 25, *Unfair Competition Law.*

8. *See, e.g., Ningobo Oriental Movement Ltd vs. Ningbo Yuanda Co Ltd and Li Guoqi* (1999) (Individual defendant found liable for infringement for stealing and using the plaintiff's trade secret, causing plaintiff to suffer damages of more than RMB 1,000,000. The Ningbao Dongjiang People's Court sentenced the defendant to three years in jail and a fine of RMB 200,000.)

9. National Conference of Commissioners on Uniform State Laws (1979) (amended 1985) at §2.

10. *Id.* at §3 (a).

11. *Id.* at §3 (b).

12. *Id.* at §4.

13.18 USC §1832(a)(5) and (b).

14. 18 USC §1831(a)(5) and (b).

15.18 USC §1834

16.18 USC §1836

17. *See* Judge Liu Yong of the Beijing First Intermediate People's Court ("[A] confidentiality agreement does not have a time limit, unless the trade secret has been made known to other people or entered into the public domain."). *See also Heilongjiang Paper Research Institute vs. Xiao Huijun, Harbin Tiangao Hitech Co. Ltd et al* (1997 Mudanjiang Intermediate People's Court).

18. See *Beijing Jianye Engineering Software Designing Institute vs. Gao Xiaojun, Hu Hanjun, Chen Wei, et al* (1998 Beijing Higher People's Court) (finding that although employers may enter into non-compete agreements with its employees, the agreement at issue had not provided the necessary economic compensation for the employees, who were therefore not bound to honor the covenants).

About the author:

Jeffrey J. Zuber is a Partner of Zuber & Taillieu LLP.

Zuber & Taillieu LLP is a high-end law firm head-quartered in Los Angeles, California, USA. Zuber & Taillieu LLP services a wide range of clients throughout the world, ranging from large public companies to individuals, conducting business in technology, financial, manufacturing, real estate, clothing, foods, education, entertainment and other industries. Its attorneys all possess law degrees from top-tier law schools, and are extensively experienced in intellectual property, corporate, finance, real estate, immigration and other areas of practice. Thus, positioned at the cutting edge of law, Zuber & Taillieu LLP is prepared to aid its clients in thriving in an increasingly competitive international marketplace.