The Challenges of Protecting Trade Secrets in China

Laura Wen-yu Young
Wang & Wang LLP

Trade secrets protection is appropriate in China, where a patent will provide an insufficient term of protection. Patents may provide a period of protection that is too short or may take too long to effect. For example, it may take five or seven years to obtain patent protection, and the product or process containing the secret may become obsolete in that time period. In the opposite case, where the product will continue to be valuable for decades after a patent would expire, patent disclosure would unnecessarily terminate the value of the secret process, and so trade secrets protection is desirable.

Statutory Provisions

China has provided protection for trade secrets since 1993,¹ but in November 2017, China’s Anti-Unfair Competition Law (AUCL) was amended to strengthen protection of trade secrets.² The article of the Revised AUCL defining “trade
secrets” is essentially consistent with article 39.2 of the TRIPS Agreement, which defines such information as valuable due to its secrecy from persons in the community of those who would be expected to have such knowledge. The Revised AUCL defines trade secrets as “technical or operational information,” “not known to the public,” having “commercial value,” protected by measures to ensure confidentiality. This is very similar to the TRIPS Agreement definition of commercially valuable information or technology. Amendments to the law also specifically address the occurrence of employers that encourage new employees to steal business secrets from their former employers.

The text of article 9 of the Revised AUCL reads:

Business operators shall not commit the following acts of infringement of trade secrets:

(1) obtaining the trade secrets of the right holder by theft, bribery, fraud, coercion or other improper means;

(2) disclosing, using or allowing others to use the trade secrets obtained by the previous means;

(3) disclosing, using or allowing others to use the trade secrets they have in violation of an agreement or in violation of the rights holder’s requirements for conserving trade secrets.

If a third person knows or ought to know that the employee, former employee or other unit or individual of the trade secret holder has implemented the illegal acts listed in the preceding paragraph and still obtains, discloses, uses or allows others to use the trade secret, it shall be deemed to infringe the trade secret.

The term “trade secrets” as used in this Law refers to technical information or business information that is not known to the public, has commercial value, and is subject to appropriate secrecy measures by the rights holder.

The amended law also increases penalties for trade secret violations. The Revised AUCL provides that where neither the actual damages to the rights holder nor the profits obtained by the trade secrets infringer can be determined, a court should adjudicate compensation in an amount of less than RMB 3 million (approximately USD 440,000) based on the circumstances. This is a significant improvement over the prior statute, which specified a maximum of RMB 200,000 in damages.
A contract designation of information as a trade secret, even though mutually agreed to by the parties to the contract, is not dispositive. Information that can be known from the characteristics of the product itself, or that is based on publicly known facts, is not protectable. Information such as price, product quality, and other characteristics that are available to the public or known to the industry or potential customers, such as product features or other potential customers, does not qualify for protection. The statute does not provide specific details or examples, but guidance to interpret the statute comes from the Supreme People’s Court.

**Interpretations and Guidance**

According to an Interpretation issued by the Supreme People’s Court in January 2017, when determining whether someone’s specific information qualifies as a trade secret, one factor to consider is the extent to which that information is of common knowledge to someone in the particular related technical or economic field. Another factor is the amount of labor and financial resources expended on developing the information in relation to the resources expended to maintain the secrecy of the information. The Interpretation also states that the commercial value must bring real or potential economic benefits, or competitive advantage, from secrecy. The Interpretation provides the example of a customer list and states that customer lists must contain more than just publicly known information such as customer names and addresses in order to qualify as a trade secret. In other words, the selection of customers is not itself sufficient to qualify the list as a trade secret. It is possible that a good argument can be constructed that a list was based on selection and criteria not obvious to others. In order to qualify as trade secrets, such customer lists cannot simply list the customers and their contact information; the list must also contain additional, non-public information, such as customer habits, tendencies, preferences, and purchasing history. The test for whether such information is non-public must be objective. Parties to a contract with trade secrets protection provisions should be careful to ensure that the nature of the information is not described in a way that allows the other party to argue that the information was already publicly known or knowable.

The statute does not define the measures an owner must take to maintain secrecy. In 1998, the State Administration for Industry & Commerce of the People’s Republic of China (SAIC), which regulates commercial enterprises, issued guidance on interpreting the statute. This guidance states that such efforts include such basic actions as marking documents “Confidential” and requiring employees...
to sign confidentiality agreements. The statute does not specify detailed steps for protection by the owner of any trade secret. In 2007, the Supreme People’s Court provided additional guidance:

In case of any of the following normal circumstances that is sufficient to prevent the divulgence of any classified information, it shall be ascertained that the obligee has taken the following confidentiality measures: (1) To limit the access scope of the classified information. . . . (2) To take such preventive measures as locking the carrier of the classified information up; (3) To tag a confidentiality sign on the carrier of classified information; (4) To adopt passwords or codes on the classified information; (5) To conclude a confidentiality agreement; (6) To limit visitors to the classified machinery, factory, workshop or any other place. . . .

**Enforcement**

The Revised AUCL provides for remedies in the event of infringement, recognizing economic growth in China requires larger penalties for deterrence. In another improvement in the statute, government authorities may order an injunction against infringement of trade secrets and also may impose a fine of between RMB 100,000 and RMB 500,000 (approximately USD 15,000 to USD 73,000). Furthermore, where the circumstances are deemed serious, authorities may impose a fine of greater than RMB 500,000 but no more than RMB 3 million (approximately USD 100,000).

The Revised AUCL provides specific authority for government agents to inspect a business site for evidence of trade secrets theft. It also grants authority to attach and seize property related to trade secrets theft and to inspect bank accounts involved in or related to such theft.

The owner of a trade secret may take action to enforce its rights by requesting that the local Administration for Industry and Commerce (AIC) protect the trade secret and bring action against the violator of the trade secret. The trade secret owner must provide:

1. a complaint including information to identify the trade secret; information on the owner of the trade secret; information on the infringing party; and a detailed allegation of the circumstances and facts proving the infringement;
(2) the domestic or foreign business license, or identification papers of the trade secret owner;
(3) business registration information on the infringing party;
(4) evidence proving the ownership of the trade secret;
(5) evidence proving the existence of the infringement; and
(6) an executed, notarized, and legalized power of attorney, as well as other documents as requested by the AIC.

There is no specific provision on time limits for action by the AIC. Generally, it takes several months to a year for the AIC to complete the entire procedure, from investigation, to hearing, to issuing a decision.

The initial hurdle to enforcement of trade secrets is the satisfactory identification of the trade secret. Sufficient detail must be provided to authorities so that the enforcement request does not exceed the scope of proper protection. But excessive specificity could result in disclosing the secret, thus forfeiting protection under the law.

The AIC, similar to other Chinese agencies, prefers that disputes be resolved by settlement of the parties. Given that China follows the civil law system and does not provide for any discovery procedure, a party wishing to file an action for trade secret infringement must have all of the evidence for its prima facie case in hand before filing the action. It is often difficult to prove a competitor is using the trade secrets, as such information is usually contained in documents possessed only by the competitor. Inferring the possession of trade secrets from the facts of a business transaction will not be sufficient proof of theft of trade secrets.

In serious cases, criminal penalties also apply. In the event of very serious losses caused by theft of trade secrets, China’s criminal law provides for a fixed-term imprisonment of not more than three years or criminal detention and/or a concurrent fine. If particularly serious harm is caused, the criminal law provides for fixed-term imprisonment of no less than three years and no more than seven years, and a concurrent fine. The terms “heavy losses” and “particularly serious losses” were initially unclear, but the Supreme People’s Court and its Procuratorate issued guidance in the form of an interpretation, which clarifies that “heavy losses” mean...
losses in excess of RMB 500,000 (approximately USD 80,000). The guidance further states that “a particularly serious result” means losses in excess of RMB 2.5 million (approximately USD 400,000).21

**Risks of Relying on Trade Secret Protection in China**

Many foreign companies have used China as a source of low-cost manufacturing for their products. China has also become the main source of assembly and production for consumer high-tech products, like computers, cell phones, activity trackers, etc. It has been well publicized that even innovative U.S. car maker Tesla will open a factory in Shanghai.22 Although the United States has imposed tariffs on a range of products from China, with more to come, cost factors still make it unlikely that consumer product manufacturing will return to the United States. If the U.S.-China trade war continues, we can expect to see production of consumer goods eventually move to other locations, such as Vietnam, even though such locations lack the extent of China’s solid infrastructure investment. Much of such production could return to Taiwan, which used to be the major source of such production and still retains significant capacity.

The foreign rights holder often does not control, or may not even know of, all the sub-vendors and contractors involved in providing its products. The extended supply chain relationships common to foreign companies manufacturing or sourcing in China are particularly unsuited to trade secret protection. While the foreign customer may be able to require its China sourcing agent or vendor to execute an appropriate confidentiality agreement, it can be extremely difficult to ensure that all of the vendor’s employees, suppliers, sub-vendors, and subcontractors, as well as all of their employees, also sign appropriate agreements or abide by the measures to maintain confidentiality of the trade secrets. In fact, one of the reasons that China is a good source for low-cost manufacturing is the flexibility of its supply chain. The best protection is to restrict access to any trade secrets to the fewest possible necessary parties and their employees, and to have each of them individually execute nondisclosure agreements or confidentiality agreements (NDAs).

If a third party without obligation learns of the information, or if the information is independently discovered or created by a third party, there is no prohibition on its use and exploitation.23 The burden is on the owner of the trade secret to maintain secrecy and to take reasonable measures to protect the trade secret. Parties obligated to maintain a trade secret are prohibited from disclosing those
secrets, and others are prohibited from obtaining trade secrets through improper means such as theft, bribery, or coercion. However, some parties allowed access may negligently fail to properly protect the trade secrets of a customer, especially in a long supply chain. If so, the trade secret would be secret no longer, and third parties would be free to make use of the information. This potential gap in coverage shows why patent protection may be favored when available.

While NDAs are essential for basic protection, they may be insufficient to protect the trade secret. It is easy to envision a scenario in which a supplier executes an NDA, marks trade secrets as “Confidential,” yet someone in the chain of control reproduces a copy of the information without the proper markings, thus allowing a third party to become an innocent recipient of the information. In that case, the use of the information is not prohibited, and the trade secret is now no longer secret. All value due to secrecy is potentially lost, if the trade secret is ultimately offered to or used by a competitor. The available relief for breach of the NDA may be inadequate compared to the loss of the secret.

If an employee receives information marked “Confidential” but leaves a copy of the information out in public, and a third party takes the information and uses it or gives it to a competitor, the trade secret is no longer secret, and the obligated party is liable for the breach committed by its agent. The party obligated to keep the information secret is liable for damages due to its loss if the trade secrets are disclosed. However, there is no recourse against the competitor, since it obtained the information through no prohibited means.

It only takes one person to release the information to others for the secret to be effectively lost. The fact that the releaser of the information may be liable for a penalty of $440,000 may be inadequate deterrence, especially in high-tech cases. A person who has a tangential connection to the entity bound by an NDA may consider the risk of a fine by the SAIC as minimal compared to the value of the trade secret. Such a person can pose a substantial disclosure risk. A foreign licensor, for example, that obtains an NDA with a Chinese supplier is vulnerable to the supplier’s employees, who may violate their confidentiality obligations. If the employees themselves did not execute NDAs, they will not have contractual privity with the trade secret owner, so the recourse will be solely against their employer. That is generally satisfactory, as the employees can be expected to be fiscally judgment-proof. The better recourse is suit against the company that executed the NDA, if the goal is to obtain damages. However, in terms of
ensuring that all vendors’ employees with access to trade secrets have an incentive to handle them with care, it is prudent to require NDAs with as many individuals as possible.

**Litigation in China**

Another important factor is the difference between the U.S. system of litigation and litigation in China. Most significant is that there is no discovery system. The Supreme People’s Court issued an interpretation of provisions of the Civil Procedure Law issued on December 21, 2001, providing that the parties to litigation are responsible for producing evidence to prove their own allegations, or to rebut the other party’s allegations. There is no system of mutual, voluntary exchange of documents, and no system for pretrial depositions. Potential plaintiffs might not obtain more information at trial than they have in hand when filing a complaint, so it is important to build a complete case before initiating the case.

While a civil claim can be filed for damages, proving damages without a discovery system can pose serious challenges. And while criminal penalties are available, it can be extremely difficult to gather proof of the crime. It can also be difficult to compete for the attention of the Procuratorate, which will have many other crimes to prosecute.

When enforcing an NDA, it is essential to clearly define the non-public information that has been appropriated. For example, in one case in China, a U.S. company sought to enforce an NDA against a Chinese supplier that began shipping directly to the U.S. company’s customers, thereby cutting the U.S. company out of the chain of supply. The NDA stated that the U.S. company’s customer list was a trade secret. The U.S. customer sought to enforce its anti-circumvention and non-disclosure agreement in court in China. The Chinese court appeared to take the position that the terms of the anti-circumvention agreement lacked mutuality and would be unenforceable. Additionally, the U.S. company sought to assert a trade secret claim against its former supplier. The supplier took the position that large-scale buyers of industrial equipment were not numerous and were generally known in the industry, therefore the customer list did not qualify for trade secret protection. The U.S. company had to show other non-public information related to its customers in order to qualify for trade secret protection. The U.S. company was able to show that it had undertaken a detailed testing and product qualification process, whose testing results and product modifications for
each customer were not publicly known. The U.S. company established through extensive affidavits and witness testimony that its supplier had copied its testing process, results, and adjustments, as well as its inventory methods and customer billing formats.

**Defending Against Trade Secret Claims**

An employer that wishes to shield itself from future liability for trade secret theft needs to require its employees, particularly designers and engineers, to execute disclosure reports along with NDAs. Unless each employee on the design team has executed a disclosure of its prior designs and undertakes not to use those designs in its current employment, the employer may find itself liable to the employee’s prior employers for improper use of a competitor’s trade secrets. While the disclosure report will not absolve an employer who in fact actively encouraged trade secret theft from an employee’s prior employer, it will provide some level of protection to the employer that acts in good faith.

China’s Revised AUCL, in the section on trade secrets, specifically addresses the situation in which an employer hires someone for the value of trade secrets that individual will bring from his or her former employer in violation of the individual’s former employment agreement. Where an employer knows that confidential information was obtained in violation of confidentiality measures, but still allows the use of that information, the employer will be liable. However, where a customer chooses to follow a terminated employee rather than continue to do business with the former employer, the new employer or the employee may avoid liability by proving that the customer voluntarily chose to work with the employee rather than his/her old employer. A noncompetition agreement with an employee must be supported by additional compensation for the period in which the employee is required to refrain from working in his or her special field. Without additional reasonable compensation, the noncompetition provision may be ruled invalid and unenforceable. Such provisions are typically included in the employment contracts of high-level managers or specialist technicians, but not for ordinary employees.

**Recent Developments**

Unlike U.S. court cases, which are matters of public record and heavily reported by U.S. media, Chinese court cases are not as well known, and there is
no system of public case reporting. However, some of the more progressive courts are posting summaries of cases on their own webpages. Nationwide, there have been over 100 cases involving a claim of trade secret protection posted on Chinese court webpages. A few recent cases from China and Taiwan are noted below. The Taiwan cases are noteworthy because of the amount of money involved. While Taiwan actions have no legal effect in mainland China, due to the close cultural connections, they will may be known and have influence on employers and employees in China.

In a recent case, China tech giant Tencent won a judgment of more than RMB 19.4 million (approximately USD 3 million), plus a return of all employee stock issued to a former employee who set up his own competing game company in 2014 prior to leaving Tencent’s employment. The employee, who had signed an NDA upon joining Tencent in 2009, had managed online game operations. Tencent later claimed that a new online game appeared and functioned very similarly to a game that the former employee had managed for Tencent. Tencent sued the former employee for more than 23 million yuan. The court of first instance issued judgment for Tencent, and awarded damages of RMB 3.72 million. Both parties appealed, and the court of second instance ruled that the employee was required to return all of his income from appreciated stock awarded by his former employer, in accordance with the nondisclosure agreement, and pay the RMB 19.4 million (approximately USD 3 million) in damages to Tencent.

In another recent case, Honghua Group Limited, maker of direct-drive top drive systems, sued a former employee and two of his collaborators for stealing its trade secrets. Honghua alleged that the two collaborators conspired to entice the employee to use email and a USB drive to provide them with Honghua’s plans and other confidential information, which they then used for their competing company. Honghua alleged the theft resulted in losses of RMB 2.5 million (approximately USD 366,000). The three defendants were sentenced to prison for nearly two years, plus RMB 60,000 (approximately USD 9,000) in fines each.

Three recent Taiwan cases were highly publicized. In December 2017, the Taiwan Intellectual Property Court issued a damages award equivalent to USD 50 million, a record for the court. The plaintiff, Largen, a Taiwan company making optical lenses, sued its competitor AOET, which had hired four of Largen’s former employees. The court found that the four employees misappropriated confidential technology related to automation processes for lens manufacturing and gave that
technology to AOET when they were hired. AOET then obtained patents on the technology. The court found AOET’s general manager and its registered responsible representative guilty along with the four specific employees who took the trade secrets. The court granted a permanent injunction and assigned the patents to Largen, but noted that AOET had caused irreparable harm by filing patents, since the secrecy could never be recovered. Finding that Largen’s research and development costs exceeded NTD 0.6 billion, the court found Largen’s damages claim of NTD 1.5 billion in lost profits to be reasonable, even though the amount exceeded AOET’s total equity.

The second high-profile case involved a former employee of chipmaker Taiwan Semiconductor (TSMC). The employee was hired by mainland company China Semiconductor (CSCMC), but was investigated and indicted before leaving Taiwan. The case is being watched as part of a large number of employee defections from Taiwan companies to mainland China companies. For example, over fifty engineers from Nanya Technologies, Taiwan’s largest DRAM chipmaker, have left for employment in mainland China, reportedly at salaries up to five times normal rates, according to media reports. U.S. chipmaker Micron also has a substantial presence in Taiwan and plans to hire 800 new workers this year to counter Chinese poaching.

In May 2016, Lao Gan Ma, a Chinese maker of black bean chili sauce, discovered a similar product released by another company and filed a complaint with the local public security bureau. After investigation, the police focused on Mr. Jia, a former technician and engineer, who worked for Lao Gan Ma from 2003 to 2015. The police confiscated the hard disk drive from Jia’s computer and found it contained confidential information of his employer, Lao Gan Ma. Jia had previously signed a nondisclosure agreement with Lao Gan Ma, but using an alias to work for another food manufacturer, handed that manufacturer Lao Gan Ma’s secret formula. Jia was arrested for infringing trade secrets. Further disposition of the case is not part of the public record.

Prior to 2016, there were two notable cases publicized in short abstracts on Chinese court websites. The first case below was heralded as the first time the amended 2012 civil procedure law was used to preserve evidence in a trade secret case. The second case below was notable for a record-high damages award and penalties, with a total of RMB 37 million (approximately USD 6 million).
Eli Lilly’s Chinese subsidiary sued a former employee for theft of computer files containing trade secrets. Lilly was able to prove that the employee downloaded forty-eight computer files to a personal device, and that twenty-one of the files contained information that qualified as company trade secrets. The employee has signed a confidentiality agreement not to use the information or to delete the files. However, the employee violated the agreement. Lilly then moved to terminate the employment relationship and five months later filed suit against the employee. Lilly moved for a preliminary injunction and evidence preservation against the employee and posted the required bonds with the court. As part of that motion, Lilly had to identify and submit information on the contents of the trade secrets. This is a step most trade secrets owners are reluctant to take, but it cannot be avoided if the owner wishes to take legal action. Since there is no pre-trial discovery system, Lilly’s only means to preserve and obtain evidence held by the defendant was to pay a bond and ask the court to enforce an evidence preservation order. The Shanghai Intermediate Court issued the preliminary injunction and evidence preservation orders against the employee to prevent disclosure or use of the protected secret information.

Of greater significance and public education is the criminal case brought against Jiangxi Yi Bo Electronics, its founder, and three other individuals. The four individuals—former employees of Saina—used their knowledge of pricing and distribution channels to undercut their former employer. Saina was able to prove that the information was protected by contract, that the contract was reasonable, and the information qualified as trade secrets. The Zhuhai Intermediate Court, located in Guangdong Province, issued orders that Yi Bo, the main corporate defendant, pay a penalty of RMB 21.4 million (USD 3.2 million) and that another corporate defendant that had distributed the products pay a penalty of RMB 14.2 million (USD 2.3 million). The Zhuhai court also ordered that the four individual defendants be sentenced to imprisonment and face monetary penalties. The company’s top leader was sentenced to six years’ imprisonment and ordered to pay RMB 1 million. The company’s second-in-command was sentenced to three years’ imprisonment and ordered to pay a penalty of RMB 200,000. The other two founders of Yibo both received a sentence of two years’ imprisonment, commuted to three years of probation, and were ordered to pay a penalty of RMB 100,000 each.

Since Guandong is a province with a high proportion of manufacturing, and Zhuhai is a port from which a large proportion of China’s exports originate,
the judgment may signify that the local culture is shifting towards greater protection of trade secrets and away from a fear of hampering China’s export and manufacturing industries.

**Conclusion**

For technology that will be utilized by only a small number of people, for several decades, or only for a short period of time commencing immediately, trade secret protection may be appropriate. If so, it must be properly documented and carefully guarded by reasonable measures at all times. If any of those factors cannot be ensured and maintained, trade secrets are best left at home and not brought into the Chinese market. The nature of the Chinese market, with its many players, and flexible, shifting supply chains, creates additional risk. When coupled with the lack of a litigation discovery process and the difficulty in obtaining evidence to prove actual damages, trade secrets become much more difficult to protect than a state-created rights like patents or trademarks.

Laura Wen-yu Young is Managing Partner at Wang & Wang LLP, where she supervises a coordinated practice handling cross-border transactions, investment, and IP matters between the West and China & Taiwan. She is also a professor of law at Soochow University, Kenneth Wang School of Law, in Suzhou (Jiangsu Province), China. A version of this article has been published in the course materials for Trade Secrets 2018: What Every Lawyer Should Know.
NOTES


3. Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994) [hereinafter TRIPS Agreement]. Article 39.2 describes such protectable information as information that “is secret in the sense that it is not . . . generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; . . . has commercial value because it is secret; and . . . has been subject to reasonable steps . . . to keep it secret.” Id. art. 39.2(a)–(c).

4. Revised AUCL, supra note 2, art. 9.

5. See TRIPS Agreement, supra note 3, art. 39.2.

6. Revised AUCL, supra note 2, art. 9.

7. Id. art. 17.

8. AUCL, supra note 1, art. 25.

9. Interpretation of the Supreme People’s Court on Some Matters About the Application of Law in the Trial of Civil Cases Involving Unfair Competition, Fa Shi [2007] No. 2 (Jan. 12, 2007) (China) [hereinafter Interpretation], https://wipolex.wipo.int/en/text/182407. Supreme People’s Court interpretations are essentially advisory opinions providing guidance to lower courts in China.

10. Id. art. 9.

11. Id. art. 11.

12. Id. art. 13.


14. Interpretation, supra note 9, art. 11.

15. Revised AUCL, supra note 2, art. 21.

16. Id. art. 13(1).

17. Id. art. 13(4).

18. Id. art. 13(5).

20. *Id.*
23. *See Revised AUCL, supra* note 2, art. 9.
24. *Id.* art. 9(1).
25. *Id.* art. 9(3).
27. Revised AUCL, *supra* note 2, art. 9.
30. *Id.* art. 24.
36. *Id.*
aspx?lib=case&id=1408&EncodingName=big5 (subscription required) (last visited Jan. 4, 2019).