

Protect your secrets in China

Companies in China often find it difficult to protect their trade secrets and know-how. **Daniel Plane** explains what legal means are available

Over the past decade, more and more companies have taken their business into China, both through establishing Chinese subsidiaries, franchises and joint-venture partners, and by outsourcing production to Chinese companies for export and, increasingly, for domestic sale and distribution in China.

In doing so, these companies regularly, and sometimes casually, entrust these Chinese entities with a broad range of valuable confidential information including customer lists, internal standards, manufacturing processes, know-how, information on sources of goods, recipes, production and sales strategies and details on tenders. Broadly referred to under Chinese law as trade secrets, much of this information is not able to be fully protected by invention or design patents, copyrights or other forms of intellectual property. That does not render it any less valuable; it merely makes it more difficult to effectively protect.

China's laws on trade secret protection

Protection for trade secrets in China is primarily enshrined in the PRC Anti-Unfair Competition Law, effective December 1 1993. The transfer of some trade secrets may also be deemed technology transfers depending on the nature of the information at issue, and therefore also subject to government regulations on such transfers. These are beyond the scope of this article.

The basics

Under Article 10, paragraph 3 of the Anti-Unfair Competition Law, trade secrets are defined as:

[T]echnical information and business information that is non-public, can bring economic benefits to the party that has rights in such secrets, is practical, and for which the party that has rights in such secrets has adopted measures to maintain its confidentiality.

The scope of trade secrets protection has been clarified by the Interpretation of the Supreme People's Court on Issues Concerning the Application of Law in the Trial of Civil Cases Involving Unfair Competition, dated January 12 2007. For example, under Article 9 of the Interpretation, the non-public nature of the information can generally be shown by establishing that it is "unknown and is difficult to be obtained by the relevant personnel in the field". As a general rule, information that is common sense or industry practice for personnel in the relevant field, consists of simple combinations of dimensions, structures, materials and parts obtainable through direct observation after a product enters the market, is published, or can be obtained through public channels or for free cannot be deemed trade secrets.

Under Article 10 of the Interpretation, the owner of the information must show that the information has "actual or potential commercial value", that it "can bring competitive advantage" to its owner, and that it has "practical applicability".

Finally, Article 11 addresses whether the information in question was protected sufficiently by confidentiality measures to warrant legal redress – an area that case law makes clear is commonly raised by those accused of trade secrets theft. Confidentiality measures such as non-disclosure agreements relating to the protected information, the adoption of passwords or codes to restrict access, marking the documents as confidential, or other measures that limit "the scope of access of the classified information", thereby only granting access to designated individuals, are the common steps deemed sufficient under the Interpretation and the Anti-Unfair Competition Law and should be considered the minimal types of measures imposed.

The Anti-Unfair Competition Law prohibits business operators from engaging in the following activities related to others' trade secrets:

- obtaining others' trade secrets by theft, enticement, duress or "other unfair methods";

One-minute read



Every book about doing business in China will contain stories about talented employees leaving to set up copycat businesses. The tales often imply that there is no legal remedy to prevent this happening. But, even when companies doing business in China are making available information that cannot be protected using the country's patent, trade mark and copyright laws, there are still options using the Anti-Unfair Competition Law. When using this Law, following the right mechanisms and taking every possible precaution from the moment you enter China is vital to ensure successful protection.

- divulging, using or allowing another to use another's trade secrets obtained in the manner described above; or
- divulging, using or allowing a third party to use another's trade secrets in breach of an agreement or in violation of the confidentiality requirements of the trade secret's owner.

Rights owners must show that alleged infringers were "well aware or ought to have been aware" that the trade secrets were obtained or disclosed by one of the three listed unfair means.

Businesses wanting to succeed in trade secrets litigation must also prove all other statutory elements to enforce their rights effectively, save for proof that the information was "not publicly known". Similarly, they must demonstrate that the accused infringer's information is similar or substantially similar to their trade secret and that that the accused had means to access the information and used unfair means to do so. Importantly, individuals accused of trade secret theft may not rely on a defence of independent development or reverse engineering if it is established that they had knowledge of trade secrets through any of the Competition Law's listed "unfair means" (see Article 12 of the Interpretation).

Enforcing your secrets

Investigation or adjudication of allegations of theft of trade secrets can be handled by administrative, civil and criminal means in China.

Administrative complaints - halting the infringements

Administrative allegations regarding trade secrets thefts are generally filed with the Administration for Industry and Commerce (AIC) at county level or above, which are to investigate following the Provisions Concerning the Prohibition of Acts of Trade Secrets Infringement, issued by the State Administration for Industry and Commerce in 1995 and amended in 1998. The SAIC Provisions generally mirror the Competition Law's rules, and provide additional rules specific to AIC handling, including, importantly, a provision for injured brand owners to obtain an immediate AIC order halting the sale of "products manufactured by utilising the rights owner's trade secrets" (presumably including provision of services relying upon those secrets) upon written guarantee to assume liability for the order's consequences. AICs are also empowered to fine infringers from Rmb10,000 to Rmb100,000 (about \$1,455 to \$14,550) for trade secrets violations (Article 25, Competition Law).

Civil complaints - injunctions and compensation for damages

The Competition Law clearly provides for AIC and civil injunctions in trade secrets matters. These can be in force until the trade secret becomes generally known to the public or for a period corresponding to the term or scope under which the owner's related competitive advantage is protected (Article 16 of the Interpretation). In addition to injunctions, courts can also award compensation for theft or misuse of trade secrets. Generally, damages for trade secret theft are measured by either the owner's loss; or, if this is difficult to calculate, the infringer's profit from exploitation of the trade secret.

Compensation may also be obtained for "reasonable expenses" of investigations (Article 20, Competition Law). Article 17 of the Interpretation also allows calculation by analogy to the method used to determine damages in patent infringement cases. Importantly, if a trade secret theft causes the information to become known to the general public (and therefore fully devalued), damages

can be awarded for the trade secret's commercial value, based upon such factors as associated R&D costs, proceeds from implementing the secret, potential benefits, and the time the secret would have permitted its owner to maintain a competitive advantage (Article 17, paragraph 2 of the Interpretation).

Criminal complaints - assessing loss

Criminal liability may be assessed for trade secret theft, though only where the loss to the injured party is at least "significant", which involves a loss of more than Rmb500,000 (\$72,750) (see Article 7, Paragraph 1, PRC Supreme People's Court's Interpretation of Several Issues on Specific Application of Law to Treatment of Criminal Cases of Intellectual Property Infringement, December 22 2004). In such cases, infringers may be imprisoned for up to three years and/or fined. If the theft's consequences are "particularly serious," such as involving a loss of more than Rmb2,500,000 (\$363,000), infringers may be imprisoned for between three and seven years and fined (Article 219, PRC Criminal Law and Article 7, paragraph 2 of the Interpretation on Criminal Cases).

Practical issues when disclosing trade secrets

While trade secret protection is available in China, the path to obtaining it can be evidence intensive and time consuming. This makes planning in advance for the risk that trade secrets will be stolen – and putting mechanisms in place to quickly identify and respond to such thefts – vital. This will not only minimise the risk that those secrets will be stolen or leaked. It will also aid in formulating a rapid and effective response to suspected breaches or thefts.

Get the agreement right first time

First and foremost – and, crucially, prior to any disclosure of information to third parties (even the company's own employees in China) – is the establishment of a clear, easy-to-understand trade secrets policy relating to the classification and handling of materials rightfully deemed "confidential" and cataloguing those materials. At a minimum, this policy should provide for such things as secure handling of trade secrets, marking of confidential materials, limiting access to parties with a need to know, and password protection of documents. Additionally, rights owners will need to create standard confidentiality/non-disclosure agreements to be signed by any parties to be granted access to those trade secrets, either independently of, or as part of employment contracts in, China. Any such agreement must take into account both the company's underlying trade secrets policy, as well as all relevant provisions of PRC law. Particular attention should be paid to the 2007 version of the PRC Labour Contract Law, which includes provisions directly affecting confidentiality and non-competition clauses in labour contracts between employers and employees.

Documents relating to trade secrets policy should also be in both English and Chinese to ensure that Chinese parties are able to understand the materials and to ease admissibility in any civil actions in China's courts. Keep in mind that these documents will not only govern relationships with Chinese employees and partners; they will be used by courts or officials to determine whether the theft or misuse of trade secrets by a China-based entity is actionable. Getting them right the first time is key.

As part of standard procedures, Chinese parties should also sign a separate bilingual document, with both non-disclosure and non-com-

On managingip.com

Politics and IP in China explained (October 2008)
Avoid China's red tape evidence trap (December 2006/January 2007)
Keeping secrets (November 2007)

Lessons to be learned

1) *General Electric Company, General Electric (China) Co Ltd and GE Healthcare (Shanghai) Co Ltd v Xi'An Jiuxiang Electrical Technology Co Ltd & Wang Xiaohui.* This case involved the misappropriation of GE's advanced repair and maintenance materials for their CT scan machines by Wang, a former GE engineer who started his own CT scan machine repair company, Jiuxiang. In the lawsuit, Wang claimed that he had not personally obtained the materials during his time with GE, that GE failed to take sufficient measures to protect the information, and that the information was publicly known. The court rejected these arguments, finding that the material used by Wang and Jiuxiang was similar to GE's materials, and that GE's measures to protect the material, including (a) a non-disclosure, non-compete clause in Wang's employment contract, and a similar agree-



ment executed by Wang upon his departure; (b) GE's marking of the compact disc and the materials thereon as "confidential" (while another disc containing basic repair manuals was not) were sufficient protective measures. The Court also found that it would be impossible to obtain these materials through public channels.

GE was awarded compensation of Rmb500,000 (\$73,000) for the trade secrets theft (as well as Rmb400,000 (\$58,500) for attendant copyright infringement), with the court using a complicated mix of the Jiuxiang's fees for its services versus GE's fees, the number of seminars conducted by the company and other relevant issues.

2) *Beijing Aozuo Ecology Instrument Co Ltd v Zhai Song.* In this case, Zhai Song, an ex-employee, was unsuccessfully accused by Aozuo of misappropriating trade secrets and passing details on to her new employer in

the form of Aozuo's confidential information regarding its dealings with its client, Nanjing University; and details on pre-tender estimates for its bid on a Nanjing University contract. The court held the information in question was not trade secrets, as Aozuo had only conducted three transactions with the university, undercutting its claims that it had developed the information over a significant period of time or at great expense or effort. Moreover, the defendant was able to successfully show that much of the information was accessible via the University's webpage explaining the bidding process. The court also rejected Aozuo's claim that Zhai Song knew of its tender estimate, generally finding that there was no evidence she was involved in preparing her new employer's tender, and that although there were similarities between that company's tender and Aozuo's, such similarities existed for all tenders for the university's bid.

petition provisions upon their termination or departure. The document should acknowledge their responsibilities under the original trade secrets policy, verify their compliance with the company's trade secrets policy and their return of any confidential materials, and commit them to not disclosing any of the company's trade secrets to any third parties nor to using any trade secrets or other information to which they had access during their employment to compete with the company or assist others to do so. Consistent monitoring of ex-employees' activities after their departure is also vital, given that their next job is likely to be with or as a competitor.

Relationships with third-parties

Third-party Chinese entities to whom companies reveal trade secrets, such as overseas equipment manufacturers or authorized distributors, provide additional challenges, given that disclosed trade secrets will be used at locations and by individuals outside the rights owner's direct control. Accordingly, potential partners should be carefully vetted in advance to ensure not only that they are willing to execute and abide by a company's trade secrets policy – but that they are able to do so to exactly the same degree as the company's own employees. To do so, companies would be wise to prepare a detailed checklist, formulated around their trade secrets policy, against which to gauge potential partners. A thorough on-site survey of the factory's facilities using the checklist should be conducted to ensure the company's trade secret policy can be executed.

Companies should also consider undertaking undercover investigations of any potential partners to gauge their willingness to violate the IP rights of others – a clear sign that they would also be willing to misuse or abuse the trade secrets of their partners. Once the relationship is underway, companies should also conduct frequent unannounced audits of these locations to ensure day-to-day compliance with trade secrets policies, as opposed only to compliance during scheduled visits.

These types of checks are particularly important where an overseas equipment manufacturer is also doing work for the company's competitors, a common occurrence in the case of larger, more sophisticated manufacturers in China. In these situa-

tions, additional security and controls must also be in place to prevent so-called cross-pollination of trade secrets or ready access to a company's confidential information by direct competitors also working with the manufacturer. For example, work spaces where confidential information is used or stored should be physically separated from competitors' spaces. Computers, phone lines, fax machines and e-mail accounts used to transmit and store information related to design, new models, production information, should be secure and well-insulated against hacking or sharing of data. Finally, employees dealing with competitors' products should be denied access to confidential information.

To the maximum extent possible, non-compete and non-disclosure agreements should be executed at the start and at the end of any relationship, both by the factory, its management, and any and all employees provided access to trade secrets. Of course, depending on the scale of the manufacturer's business and its client base, it may be difficult to prevent it working with or for competitors altogether. Nevertheless, it is reasonable to demand that confidential information, technology or other materials obtained during the relationship not be used to assist competitors.

Unlike traditional IP rights, no registration certificate establishing ownership in trade secrets is granted by the government. Instead, and in addition to establishing the alleged infringement, trade secrets owners are also required to clear a number of hurdles to establish that the information they claim as a trade secret qualifies for protection. It is vital that trade secrets owners adopt a clear, concise policy related to the protection and handling of those materials before disclosing them in China, and ensure that both its PRC employees and any third parties to whom those secrets are disclosed abide strictly by that policy. Failure to do so not only risks easy disclosure of the trade secrets; it potentially renders those secrets unprotectable, devalued, or even valueless.



Daniel Plane

© Daniel Plane 2009. The author is a senior associate with Gide Loyrette Nouel in Hong Kong