EU-CHINA IPR2 中国欧盟知识产权项目二期

Roadmap

for Intellectual Property Protection in Europe

Trade Secrets Protection in Europe

Suggested for use by companies, particularly new entrants to the EU marketplace

Prepared February 2011

This publication has been produced with the assistance of the European Union. The content of this publication is the responsibility of the IPR2 implementation team and in no way can be taken to reflect the views of the European Union or other relevant authorities in Europe. In addition, this publication cannot be taken to reflect the views of the authorities of the P.R. China.

Contents

Overview

It is essential that companies are able to create and foster the information necessary to develop new or improved goods or services to thrive in an increasingly competitive and global business environment. The information that enables a company to compete effectively is a 'trade secret' and is therefore of commercial value and worth safeguarding. Famous examples of a trade secret include the Coca Cola formula and Microsoft's source code for Windows. Competitors may gain access to such information relatively easily, for example, by winning over or merely hiring away key employees who created or have access to this confidential information. A successful company can help to safeguard against the loss of a trade secret, for example, by signing nondisclosure agreements or taking security precautions against business partners. Small and medium-sized enterprises (SMEs) in particular may not be aware of the risks as their business grows, and should develop an effective trade secret management programme and take measures to protect the trade secrets against misappropriation in form of stealing or industrial espionage. Misuse of such information (by persons other than the owner of the trade secret) is considered as an unfair practice and can be protected before the court.

Depending on the legal system, trade secret protection is integrated in the general concept of protection against **unfair competition** or provided for under specific provisions on the protection of confidential information in **contract or criminal law**. There is no uniform enforceable trade secrets law in the European Union (EU): The basic principles are similar in all 27 EU Member States but nevertheless the nonexistence of a supranational system defines different ways of regulation in each country.

This roadmap aims to give a general definition of trade secrets, their nature and scope and should help contribute to a better understanding of the practical challenges in identifying them and the various means of protecting them. The roadmap will explain what is meant by misappropriation of a trade secret and what suitable actions can be taken to prevent violation of trade secrets in different circumstances. Because of the specific regulations on the protection of trade secrets it is advised that companies check the national legislation of every EU Member State where trade secret protection is sought and to turn to regional professional intellectual property experts when developing an IP protection management strategy which includes trade secrets protection.

Importance of trade secrets protection

Nowadays the importance of trade secret protection and the development and implementation of information protection practices has increased due to the dynamic development of the business environment. As national and international frameworks of intellectual property rights (IPRs) evolve, designed mostly to encourage innovation, the regulation of trade secrets is gaining attention more than ever before. When legal protection is given to products that are the result of investment in research and development, protecting a trade secret is, in certain cases, the preferred form of intellectual property protection in the information economy.

A trade secret is different from other forms of intellectual property, in that its protection requires **good will and maintenance** and in some cases it is the most attractive, effective and readily available intellectual property right.

Distinction between patents and trade secrets

Because of their confidential nature which requires disclosure to obtain legal protection, trade secrets are not protected in the same way as other forms of intellectual property, such as patents, copyrights, or trademarks, are. Yet trade secret protection offers a much broader scope than patents, trademarks, or copyrights. A patent requires that the invention is novel, useful, and non-obvious, has been disclosed to the public, and conforms to a definition of patentable subject matter. Trademarks protect only the printed word or image referencing a product or service in commerce. Copyrights protect only the manner of expression, but not the content - the idea, information, or concept - being transmitted.

Unlike patents, trade secrets can protect unpatentable subject matter. They do not need to be novel or non-obvious. Trade secrets are protected without any registration or the fulfillment of any formal requirements or procedures to any official authority for protection. Therefore, a trade secret can be protected without limitation in time; as long as it is kept confidential.

Trade secret protection may be advisable:

- When the secret relates to a **manufacturing process or invention,** rather than to a product, as products would be more likely to be reverse engineered and can therefore be protected as a trade secret;
- When the trade secret is **not considered to be of such great value** as to be considered worth a patent;
- When the secret is **not patentable**;
- When it is likely that the information can be kept secret for a **considerable period of time** for over 20 years (period of protection of a patent);
- When an enterprise has applied for a patent and **is waiting for the patent** to be granted. For example, in some countries an invention must be kept as a trade secret until it is decided whether to continue to keep it further as a trade secret or to patent it.

However, trade secret protection is generally weak and more difficult to enforce. Trade secret protection only protects against improper acquisition, use or disclosure of confidential information. If the secret is disclosed, anyone may have access to it. The disadvantages of trade secrets are also high costs connected with the implementation of the safety and information protection policy, control, surveillance. Furthermore others may discover it independently or may patent it.

If the trade secret is patentable know-how, it should be carefully assessed before deciding whether to patent the invention or to keep it secret. The proprietary company must consider what kind of know-how is involved, its contemplated use, the term of the expected competitive lead and the capability to ensure secrecy for a longer period. For these reasons trade secrets protection may appear particularly attractive to an SME.

Legal framework governing the protection of trade secret

The EU system for trade secret protection is not totally harmonised. TRIPS and other international acts give just minimal legal standards for trade secret protection, leaving individual countries enough room to approach the issue themselves. EU law is based on these principles, but has not addressed the issue directly. Therefore, SMEs should be aware of those potential differences.

International Trade Secrets Protection

The Paris Convention

The **Paris Convention for the Protection of Industrial Property** of 20 March 1883 can be found on: http://www.wipo.int/treaties/en/ip/paris/trtdocs_wo020.html#P19_137. It prohibits unfair trade practices among its members; meaning "[a]ny act of competition which is in conflict with the fair customs of industry and trade" is unacceptable. The examples of unfair competition provided by the Paris Convention do not explicit mention trade secrets infringement. But it could be argued that industrial espionage or other unfair means in the sense of trade secret is considered as unfair competition under the Paris Convention terms.

TRIPS

The **Agreement on Trade-Related Aspects of Intellectual Property Rights** (TRIPS) is based on the substantive provisions of the Paris Convention for the Protection of Industrial Property and the Berne Convention for the Protection of Literary and Artistic Works and can be found on: http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm.

The most relevant provision of TRIPS is Section 7: Protection of Undisclosed Information. Article 39 (2) states:

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:(a) 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;

(b) has commercial value because it is secret; and

(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

Another relevant TRIPS characteristic is its provisions on IPR enforcement. Members must ensure fair and equitable enforcement procedures to IP right holders, including sufficient authority to require the production of evidence, and remedies such as injunctions and compensation for damages.

The legal standards for trade secret protection as well as other IPRs protected by TRIPS are subjects of the WTO's international dispute settlement system.

European Trade Secrets Protection

The EU does not have any specific legal provisions to protect trade secrets or undisclosed information although the laws in various European countries have long standing traditions of protecting trade secrets. Some EU Member States like Italy, Germany and Bulgaria provide strong protection for trade secrets. Injunctive relief, damages and third-party liability available to the private litigant exists in France, Germany, UK and etc. Generally, most of the Member States do not have a specific law for trade secrets. Depending on the legal system, the protection of trade secrets is based on specific provisions on the protection of confidential information, on the protection against unfair competition, as well as on other provisions in contract and criminal law. For example:

- **contract law**, when the agreement between parties seeks to protect the trade secret by using a non-disclosure clause or confidentiality clause, through an anti-reverse engineering clause, etc.;
- **law against unfair competition**, when misappropriation is done by competitors who have no contractual relationship or indulge in an act of theft, espionage;
- **criminal law**, when an employee steals trade secrets from a company or is involved in acts that may be considered as invasion of privacy, electronic espionage, etc.

The status and the form of protection of trade (business) secrets, including know-how, and the treatment of acts of unfair competition is very different among Member States. On the European level a company can apply the European **IPR Enforcement Directive** (Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights) only if the trade secrets are protected as an intellectual property right at national level. The IPR Enforcement Directive gives the procedural provisions, concerning any infringement of the intellectual property as provided for by Community law and/or by the national law of the EU country concerned. This Directive contains substantial provisions and covers the remedies that are available in the civil courts, but not criminal

offences. The Directive can be found here:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:157:0045:0086:EN:PDF.

What is a trade secret?

Based on the TRIPS Agreement a trade secret is commonly defined in broad terms in many countries as any information, including but not limited to, technical or non technical data, a formula, pattern, compilation, programme, device, method, technique, drawing process, financial data, or a list of actual or potential customers or suppliers that:

- is sufficiently secret to derive economic value, actual or potential, from the fact that it is not generally known to other persons who could obtain economic value from its disclosure or use; and
- whose secrecy is achieved thanks to its holder's reasonable efforts.

Trade secrets have three main elements: the information must be **secret** in itself, it should have **economic commercial value**, and the holder must show **reasonable efforts** steps to keep the information secret (e.g. confidentiality agreements). These principles have been long recognised in the EU Member States.

A trade secret is a process or device for continuous use in business operations and important and/or critical to the functioning of a company. These are technical, technological and manufacturing secrets. The following offers an idea of the broad range of what these could be:

- data compilations, for example lists of customers (the more information a list contains, the more likely it is to qualify for trade secret protection), list o f special suppliers
- designs, drawings, architectural plans, blueprints and maps, instrument, pattern
- valuable business information such as business strategies, methods of doing business and marketing plans, for example a company's plan to launch a new product, business plans;
- costs and price information, purchasing price of raw materials
- information about research and development activities
- even negative results, for example R&D efforts, may form part of trade secrets as they are of significant value, when not known to competitors. Some other examples of negative results may be details of failed efforts to remedy problems in manufacture of certain products, research ideas, projects abandoned or given-up, failed marketing strategies, etc.
- algorithms and processes that are implemented in computer programs, and the computer programs themselves, software, source codes
- manufacturing technology (details) or repair processes and techniques; process details
- document tracking processes
- schedules, manuals, ingredients, sketches, engineering drawings
- prototypes
- product characteristics
- formulas, practice, process
- salary structure of a company, compensation packages
- strategic promotional or marketing material under development
- know-how
- test data, laboratory note books
- distribution channels
- agreements containing details of marketing tie-ups

While it is not possible to precisely define a trade secret, courts often consider a non-exclusive list of factors to determine whether information is, in fact, a trade secret. These

factors are:

1. Extent to which information is known outside the SME.

2. Extent to which the information is known by employees and others involved in the SME.

3. Measures taken to guard secrecy of information.

4. Value of information to a business and its competitors.

5. Amount of effort or money contributed by the owner developing information.

6. Ease or difficulty with which information could be properly acquired or duplicated by others.

Secrecy

Information that is the subject of trade secrets should be confidential. Information is secret when it is **not generally available to the public or readily accessible**. It happens that apart from its owner, persons other than the owner may know of the secret. However if this disclosure was confidential (for example to employees or business partners) or bound by secrecy, this will not destroy the status of the trade secret.

Economic value

The second element is the economic value of the trade secret to the business. The trade secret economic value factor is interconnected with the element of secrecy. The value of a trade secret should be significant and provide some sort of economic benefit to the company.

Reasonable steps to insure the secrecy of information

The third element includes the reasonable steps to keep the information secret. This element is also a very important feature. During the lawsuits the courts examine whether or not the owner of the information has taken **necessary and reasonable precautions** to safeguard the information. This means that it is up to the claimant of the trade secrets to show that he has a secrecy policy, within its normal business procedures. This can be some form of marking of the information as "Confidential", some restricted access to that information, perhaps provisions in its employment and other agreements dealing with this information and etc. However there must be a **written policy** in effect regarding disclosure to employees and others, that defines what the information is and how and under what circumstances it can be used and by whom. The written policy demonstrates guarantee to protection which plays an important role in litigation.

Protection of trade secrets

What measures should be taken by businesses to protect their trade secrets?

Even though it has been stated that the EU lacks uniform trade secrets protection standards, legal protection is generally sought by taking steps to stop or prevent the trade secret from being improperly acquired, disclosed or used by others who are either automatically bound by a duty of confidentiality (including employees), or by people who have signed non-disclosure agreement, or even by people who acquire a trade secret through improper means (such as theft, industrial espionage, bribery), etc.

The owner of a trade secret should take measures to protect and maintain its **confidentiality**. A common way of doing so is to include **confidentiality agreements within employees' contracts**, sign nondisclosure agreements with employees during and after employment, and also oblige them not to use the trade secret for competition purposes (e.g. with a view of running their own competitive business); as well as sign **confidentiality agreements with business partners** whenever disclosing confidential information with licensees and financial partners. In order to restrict access to the information, **technical means of protection** can also be applied: It is recommended that a company undertakes physical security measures such as periodic security checks, closed-circuit monitors, monitoring or restricted access to computer-stored data and restricted access to computers and classified areas.

Employees

Educate employees on issues related to information security

During the course of the employment relationship, employees must be made aware of their **fiduciary duty** to protect confidential information and be periodically educated about situations that may result in the disclosure of trade secrets. **Employee education** must be an integral part of any trade secrecy programme. An employee who has legitimate access to an employer's trade secret has to treat that information with great care. For this reason there should be processes in place for notifying employees of the company's trade secret rights and for protecting trade secrets as they are used in the company's business operations. Education on issues related to information security makes trade secret protection part of the enterprise culture and trains employees on information security policy. Training and awareness are without a doubt the most cost-effective aspects of any protection programme.

Mark documents and restrict public access

Another measure to be taken in order to protect trade secrets is **restricting public access** to the confidential information. It is necessary to limit the information to key personnel and only on a need-to-know basis. Protection of trade secrets can also be achieved by limiting access to the archives or other rooms where confidential papers are stored and to restrict the access control through appropriate authorisation. Physical restrictions, especially regarding visitors and other outsiders, which limit access to organisation facilities and to areas containing valuable information, especially trade secrets of course, are essential. In addition other measures that can be taken to restrict public access to facilities include:

- Maintain logbook and visitor's pass;
- Accompany visitor;
- Make areas visible to anyone walking through a company's premises, for example, type of machinery, layout, physical handling of work in progress, etc.;
- Password control for access, record of document accessed by employees, biometric palm readers, wherever necessary;
- Guards and surveillance cameras; overheard conversations; documents left in plain view; unattended wastebaskets.

Another good way to protect trade secrets is to clearly **mark documents,** for example as "Confidential".

Confidentiality contracts and Non-Disclosure Agreements

A nondisclosure agreement (also known as confidentiality agreement) is one of the best tools for trade secret owners to protect confidential information and help facilitate the burden of proof in case of litigation.

A nondisclosure agreement is an agreement where a party accepts a clear and explicit duty not to disclose or improperly use confidential information that has been shared with him.

These agreements typically cover an **extended period** of time - thus, an employee who executes a nondisclosure agreement agrees not to use or disclose the information for a certain minimum period of time, even after the employee has left the job. For such an agreement to be enforceable, it should clearly define what information falls within its protection. Therefore, it is extremely important to maintain confidentiality or the secrecy of information with specific commercial value. An employer with valuable trade secrets should require all employees with access to those trade secrets to enter into such a nondisclosure agreement.

Under the law of many EU Member States, however, it is not always necessary to sign an independent agreement because in many countries the law governing employee-employer relations requires the employee to maintain the confidentiality without such agreements. Generally, employees are under an **implied duty** not to use trade secrets that they acquire during their employment desirable to the employer. An implicit duty is found where the circumstances of a particular situation suggest that both parties contemplated secrecy. Nevertheless, this implied duty only arises when the employee knows or should have been given access to a trade secret without signing a confidentiality agreement. If the employer informed the employee of the confidential nature of the information, and the employee understood this, courts would likely impose an implicit duty of trust and confidence on the employee, rendering them liable for trade secret misappropriation if they later use or disclose that information without the employer's consent.

However a well-prepared non-disclosure contract is a strongly recommended preventative means of dealing with employee misconduct and facilitating the burden of proof in case of litigation. A good nondisclosure agreement is detailed and direct, and limits post-employment restrictions in time and geographical scope.

Nondisclosure agreements constitute, therefore, a **cheap and effective measure of preventing employee's misbehaviour**, and should be used with vendors, contractors, prospective or temporary staff, interns, visitors, non-employees working on site and customers at virtually all levels of the enterprise whenever disclosing confidential information.

Non-compete agreements

Once the employment relationship has legally ended any form of restriction reduces the economic mobility of employees and limits their personal freedom to pursue a preferred professional course. On the new working place the employee is still potentially bound to the acquisition of supposed trade secrets; and thus he is restricted by his increased expertise from advancing further in the industry in which he is most productive. It should be noted that the general knowledge, skills and experience of a former employee cannot be restricted.

Therefore, employees leaving the company should be reminded of their continuing responsibilities and of the need to return any information or documents that may contain trade secrets. They should also sign a separate report attesting to the return of all confidential information and trade secrets. This type of a **non-compete agreement** stops the independent contractor from competing with the business or stealing its ideas.

When requiring employees to sign a non-compete agreement, the employees must agree not to work for a direct competitor for a certain amount of time after leaving the company. The rationale behind this is that over time, the trade secret may no longer be valuable or will have changed as the business advances.

In other words, the terms of a non-compete agreement must be reasonable as to the duration, territory, and scope of the activity. A **one-year time** restriction from a competitor's business is generally regarded as normal. A restraint is generally enforceable if it is designed to fairly protect the employer's trade secrets.

Monitoring employee activities

Another protective measure is to conduct **periodic information security audits**, as follows:

- Monitor compliance, prosecute violators departing employees;
- Conduct exit interviews to make the employees aware of their obligations when they leave the organisation especially in issues related to confidentiality, trade secrets, etc.
- Writing letters to new employees informing them about some aspects of areas in which the employee was involved so that the employee is not put onto such projects in the new organisation.
- Treat all employees fairly and compensate them reasonably for any IPR generated from their work.

Other security measures

The protection programme should include **efforts to identify and safeguard digital and information systems through security measures** integrated within the fully networked enterprise where intranets, extranets and the internet are used to gain competitive advantage. This could be as follows:

- Secure online transactions, intranet, and website;
- Equip the entrance to manufacturing or research and development facilities with a security pass, authorisation (password); access control;
- Physically isolate and lock: computer tapes, discs and other storage media;
- No external drives and USB ports;
- Monitor remote access to servers;
- Support internal security measures with an external monitoring and surveillance function: installation of key and encrypted computer data accesses as well as antivirus software, and the protection of e-mail communication.

Business partners

A company can keep its confidential information from competitors by requiring its business partners to sign non-disclosure agreements prohibiting them from disclosing trade secrets. Such contracts preventing disclosure may also be used when a company is engaged in **licensing or other business negotiations**.

If the business partner bound by such an agreement in the course of business negotiations discloses or misuses trade secrets in violation of the contract, he may be subject to financial penalties, usually provided for in the agreement, as well as remedies against trade secret violations imposed by the national law of the every EU Member State.

Licence agreements

Licence agreements, know-how contracts or other legal methods for the commercial transfer and acquisition of technology are important means of protecting trade secrets within the relationship between a company and its business partners.

For smaller companies, the advantages include the ability **to leverage business resources**. In this context, SMEs could more easily and more efficiently further their research and development efforts with marketplace partners instead of undertaking research and development (R&D) independently. A licensor stands in the position of being able to enter into markets that he could not have entered previously without the license. Often without sufficient personnel to deploy or utilise a trade secret, small companies and start-ups will grant licenses to **reach growth targets**.

If a company has a trade secret, it can license (i.e. lease) its trade secret to others.

Companies should take following aspects into consideration when drafting licence agreements:

- A licence permits the owner of the trade secret to impose conditions on how and under what circumstances the information is used. A duty of trust and confidence is most often created **explicitly**. For example, if a company licenses its trade secret to another party and the licence agreement contains a confidentiality provision, the licensee has an explicit duty of trust and confidence. Anytime such an explicit duty is breached with regard to the trade secret, the breaching party commits trade secret misappropriation.

- European courts have found that a party who receives trade secret information through a licence agreement has received such information **lawfully**.

- Licence agreements also include an **antitrust aspect**. The EU has strict antitrust laws that affect **technology licensing**. It has issued detailed regulations known as a block exemption, governing patent and know-how licensing agreements as well as ancillary provisions relating to other intellectual property rights. The most important are the Commission Regulation (EC) No 772/2004 of 27 April 2004 on the application of Article 81(3) of the Treaty (now Article 101(3) of the TFEU) to categories of technology transfer agreements (TTBER)[1] and the Commission Notice - Guidelines on the application of Article 81 of the EC Treaty (now Article 101 of the TFEU) to technology transfer agreements (Technology Transfer Guidelines)[2].

These regulations should be carefully considered by anyone currently licensing or contemplating the licensing of technology to the EU.

- The companies can foresee exemptions for territorial restrictions in their know-how licences until the licensed know-how is no longer secret, or, in the event that secrecy has been compromised by the licence, the length of the agreement. Licensing trade secrets requires special care, because once secrecy is broken, trade secrets may become worthless, and the licensor generally wishes to have good control over what the licensee can or should do. The companies have to clarify the question **what will be the governing law** in order to be able to draft proper licensing agreements. The SME have to be aware that the divergent trade secrets laws may create problems in the context of licensing agreements, if some confidential information qualifies for protection in one Member State, but does not in another. This could impede transfer of technology. The discrepancies in national trade secrets laws may also create barriers to trade, for example, when a product which is lawful in one country violates the trade secrets laws of another Member State. Therefore, companies should be careful of those potential differences and be prepared of the problems that can come up.

1 The Commission Regulation can be found at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0772:EN:HTML

2 The Commission Guidelines that can be found at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004XC0427%2801%29:EN:HTML

Joint venture

Licensing agreements, know-how contracts or other legal methods for the commercial transfer and acquisition of technology can be integrated into any form of **joint venture arrangement**. A joint venture is a form of alliance between two separate companies. Information may be most valuable when it is licensed to others or forms the basis for a joint venture or similar cooperative arrangement. Before entering into a joint venture or similar arrangement, the parties should negotiate and sign a detailed agreement addressing ownership and protection of confidential information.

Joint ventures typically involve two types of confidential information – information contributed by the venturers and information developed as a result of the venture. The joint venture agreement should address ownership and protection of each type of information, both during and after the joint venture. Joint ventures develop a separate business unit to allow two or more parties to work together in conducting specified business activities. The establishment of joint ventures are often considered as an opportunity for SMEs to upgrade its internal development capabilities and to acquire technical know-how from more advanced partners in more developed countries.

Misappropriation of trade secrets

Definition

Trade secret misappropriation occurs where someone acquires, uses and/or discloses a trade secret without permission and in an improper manner. Typical examples include illegal acts such as theft, bribery, or obtaining protected information fraudulently or through illegal surveillance, misrepresentation, breach or induced breach of a duty to maintain secrecy, or espionage by electronic or other means.

Trade secret misappropriation typically falls into two areas - where the trade secret is misappropriated by someone who had proper access to it (internal thefts) and where the trade secret is misappropriated by outsiders (external thefts). This is why, when transferring a trade secret, its owner should pays great attention to confidentiality provisions and to the efficiency of court injunctions that can be obtained locally to prevent unauthorised disclosure.

What are improper means for learning of a trade secret

A trade secret owner is only protected from unauthorised disclosure and use of the trade secret if the other party did not have the permission to use or disclose the information and the trade secret is either acquired through improper means or another person knew or had a reason to know that it was acquired through improper means. If they were innocent of this fact (where, for example, a third party wrongfully acquired your trade secret and sold it without letting on that it was a trade secret), that innocence can be used as a defence claim of misappropriation.

Therefore the trade secret owner can take only in these cases legal action against someone who misappropriates the trade secret, for example when an ex-employee passes on trade secrets of the previous employer to the new employer or uses the trade secrets of the previous employer in a new business or new job, if he had taken **adequate care** to protect the trade secret. It is also important to bring to the notice of employees, contractors and business partners the type of information they are bound to respect as trade secrets. Often times, people will have legitimate and permitted access to a trade secret. When someone with legitimate access uses your trade secret for his or her own advantage, or discloses it to others, they may have committed trade secret misappropriation, which means that the trade secret owner could seek legal relief from the courts. The important question about misappropriation is whether or not they had a duty of trust and confidence which they violated by using and/or disclosing your trade secret.

One of the most well-known examples of such legal-but-improper means involved a company which was building a new manufacturing plant. While the plant was still under construction, a rival company flew a plane over the construction site and took photographs of how the plant was being put together. In doing so, the rival did not break any laws. However, the original company's manufacturing process was a trade secret and the court found that the rival improperly

attempted to learn that secret by flying over the plant. The rival was therefore liable for trade secret misappropriation. The reason the court came to this conclusion was that it would be unreasonable for the original company to have been forced to cover its whole construction site while the plant was being built. The improper means used to acquire or learn of a trade secret do not necessarily have to be illegal to be found improper. If someone takes **active steps** in an attempt to overcome the trade secret owner's steps to maintain secrecy, that may be enough to constitute improper means.

While such attempts can be found to be improper, it is important to understand that there are means of learning a trade secret which are proper. The proper way for someone to learn about and use a trade secret is such as through reverse engineering a product, which does not qualify as trade secret misappropriation (meaning you have no right to sue them or get them to stop their actions). If the secret is embodied in a product it may be reverse engineered or if it was independently discovered, without using illegal means or violating any agreement, law, etc.

What is reverse engineering?

Reverse engineering is determining someone else's trade secret information by examining and testing publically available information.

Reverse engineering occurs where someone **legally obtains** a product, and then **discovers** how that product works or how it was put together by carefully studying it, taking it apart, experimenting on it, etc. Such proper means would include obtaining the information from public sources or public publications, licensing it from the trade secret owner, independently creating it, reverse engineering it, etc. Reverse engineering is a very common industrial activity, and as long as the trade secret was legally obtained, this is a proper means of learning about someone's trade secret. It is obvious that as soon as new information, products or equipment are made available on the market, competitors may analyse the process in order to understand and imitate or reproduce it. It is important to realise that trade secret is protected so long as one is able to keep it a secret. By appropriate contracts, one binds various people associated with the trade secret not to disclose it to others without explicit consent of the owner of the trade secret. However, if someone, without legal access to the trade secret information, decodes or arrives as the information using legal means, such as reverse engineering or independent invention, then they cannot be stopped from using the information. Under these circumstances, the owner of a trade secret cannot take any legal action.

This is one of the reasons that a patent is sometimes **preferable** to a trade secret. Even if someone reverse engineers a patented product, they cannot use it without the patent owner's permission. However, they are free to use a reverse engineered trade secret without seeking any permission from the trade secret's owner. If someone have learned of or acquired someone's trade secret through proper means, he has not committed trade secret misappropriation. Similarly, if a person received the information from someone else and did not know or have reason to know that that person had improperly obtained the information, he is not liable for misappropriation. While the trade secret owner may file a lawsuit against that person, he would not ultimately be liable for any damages. But again, this is only true if that person did not know the information was improperly obtained and he had no reason to know this.

Stealing trade secrets

Trade secrets are potentially critical area, especially in an information economy when there is high turnover of employees within a company; a more mobile workforce; increased use of contractors and consultants; and increased outsourcing of infrastructure which increases the chances of them being stolen. Valuable information and data is stored in high-density electronic media, such as CDs, USB memory sticks, etc. and, therefore, it is no longer necessary to physically carry information which this makes it easy to transport. In this way, computers have made it much easier to create and steal trade secrets. Increasingly, internet connectivity, file sharing technologies makes it more unproblematic to transmit quickly information in high volume. Combined with the increased mobility of the work force, there is a high possibility that the trade secrets can be stolen. Locking trade secrets up against outsiders is no longer enough.

Therefore, it is no surprise that today the majority of trade secret infringements are **insider thefts**. While companies go to great lengths to protect against disclosure to outsiders, it is a well established fact that more than 80 % of informa-

tion crimes come from within a company, and are linked to employees, contractors, trusted insiders and are the result of malicious destruction, erasure of R&D data by disgruntled/ dismissed employees, theft by former employees and, in several cases, due to the ignorance of obligations relating to trade secrets of current, former and retired employees. These insider thefts are preventable. Businesses can and do strive to protect their trade secrets by enacting corporate security measures and confidentiality clauses in employment, technology licensing, distributor ship and joint venture agreement. Here are some examples of the physical security measures: periodic security checks, closed-circuit monitors, monitoring or restricted access to computer-stored data and restricted access to computers and classified areas. These prevention methods are both necessary and cost-effective and help a great deal in protecting trade secrets from theft by the people to whom companies must disclose the trade secrets if they are to do their jobs: employees, vendors, and consultants.

Internal theft by disgruntled workers or former employees is also intentional. Some of these people allow themselves to be exploited by competitive intelligence operatives, for example money. Indeed, it can be said that the primary business activity of most businesses today is the creation of trade secret information - the entire range of what works and what doesn't work, what has happened in the past and what is planned for the future. Theft of these trade secrets and infringement by competitors is a direct threat to the shareholder value of the company.

Industrial espionage

Industrial espionage is another common method to misappropriate a trade secret. The industrial espionage belongs to the external threats to trade secrets of an organisation or company.

External threats include corporate spying with professional criminals targeting specific technology, initiating network attacks (hacks), laptop computer thefts accessing source code, product designs, marketing plans, customer lists, approaching employees to reveal company information, etc.

Intense competition in domestic and export markets had also lead to an alarming increase in theft by outsiders. Industrial espionage is increasing due to the global competition, shorter product cycles, thinning profit margins, and declining employee loyalty. The possibility that trade secrets are high value assets that may be used, sold or traded especially in technology-led businesses has gradually brought many companies to take reserve of their trade secret identification and management policies, programmes, procedures and day-to-day practical measures and activities. Fierce competition in domestic and export markets has also led to an increase in industrial sabotage and espionage when trade secrets may also be lost easily if proper protection measures are not put in place to cover employees, partners, web sites and physical or electronic systems owned or used by a company. With increasing competition in markets and rising cost of R&D, loss of trade secrets is gathering bigger importance.

The typical response to keeping trade secrets secure is to use better and more sophisticated ways to lock them up. Companies have enormous costs per year on such methods. Passwords, secure facilities, security guards and name badges, and internet firewalls all serve to lock trade secrets up more securely. All of these security methods protect against disclosure to outsiders.

Trade secrets are separately regulated in each of the 27 EU Member States: national authorities and laws govern their grant, scope, enforcement and validity within the national territory. Trade secrets infringements by third parties are generally considered as **torts**. In that cases when trade secrets are protected as an intellectual property right at national level, they should be understood as being covered by the scope of the EU's IPR Enforcement Directive. The companies have to take into account that the general principles of sanctions against procurement, the procedures and remedies that ensure the enforcement of the intellectual property rights on the European level are provided in the Enforcement Directive. The Directive covers all infringements of intellectual property rights without containing any definition of **intellectual property rights**. The companies have to be aware that the scope of the Directive is not limited to those rights harmonised at EU level, but also covers rights protected as intellectual property rights by national law. The Directive therefore provides only for **minimum harmonisation** as far as enforcement measures are concerned. The companies have to know the substantive law on intellectual property, Member States' international obligations (notably the TRIPS Agreement) including Member States provisions on criminal law because as a procedural law the Directive doesn't affect above mentioned.

Remedies against misappropriation/violation of trade secrets

Trade secrets are separately regulated in each of the 27 EU Member States: national authorities and laws govern their grant, scope, enforcement and validity within the national territory. Trade secrets infringements by third parties are generally considered as torts. In that cases when trade secrets are protected as an intellectual property right at national level, they should be understood as being covered by the scope of the EU's IPR Enforcement Directive. The companies have to take into account that the general principles of sanctions against procurement, the procedures and remedies that ensure the enforcement of the intellectual property rights on the European level are provided in the Enforcement Directive. The Directive covers all infringements of intellectual property rights without containing any definition of intellectual property rights. The companies have to be aware that the scope of the Directive is not limited to those rights harmonised at EU level, but also covers rights protected as intellectual property rights by national law. The Directive therefore provides only for **minimum harmonisation** as far as enforcement measures are concerned. The companies have to know the substantive law on intellectual property, Member States' international obligations (notably the TRIPS Agreement) including Member States provisions on criminal law because as a procedural law the Directive doesn't affect above mentioned.

What acts constitute a trade secrets violation or infringement?

A trade secret owner can protect himself against unauthorised disclosure and use of the trade secret as well as against its use by a person who acquires it by theft, fraud, or breach of the confidentiality obligation.

The prohibited acts may include obtaining and using trade secrets, and disclosing them to a third party without authority. Inadvertent or accidental disclosure of a trade secret to public, generally it is no longer a trade secret. It may also be prohibited to knowingly or negligently obtain or use improperly acquired trade secrets. Further the premature disclosure of commercially valuable information, including know-how, may be damaging or fatal to subsequent attempts for its protection by a patent or design registration. An invention or design can be kept as a trade secret until it is decided whether to continue to keep it further as a trade secret or to patent it or to register it as a design. In this way when a company inadvertent or accidental discloses its trade secret is, this will make the patent or design registration impossible and the company can loose its benefit.

To establish **violation of trade secret rights**, the owner of a trade secret must be able to show that:

- Infringement by or competitive advantage gained by the person/company which has misappropriated the trade secret.
- The owner had taken all reasonable steps to maintain it as a trade secret.
- There is misuse as information obtained has been used or disclosed in violation of honest commercial practices.

Litigation

Unlike patent, trademark and copyright infringement suits, trade secret lawsuits require the plaintiff to prove the existence of a trade secret, and that he has ownership rights to it. Trade secret lawsuits typically allege infringement of a large group of trade secrets. This is partially a result of the fact that trade secrets are not bound by a disclosure. Partially it is because patent, trademark and copyright infringement cases are fought to protect those intellectual properties where the plaintiff has the strongest case.

This same strategy should apply to trade secrets cases. The plaintiff should avoid alleging infringement against every trade secret that defendant had access to and may have infringed. The plaintiff lays down his strongest allegations generalising the arguments to all of the information. On the other side the defendant has been given the opportunity to argue against the weakest allegations, and generalise these arguments to all of the information. Alleging all possible infringements will seriously make the plaintiff's case weaker. It is advisable to litigate only over very specific, strong trade secrets. This will force the defendant to argue on his weakest thesis. Limiting the lawsuit to the strongest allegations has shown to be particularly relevant when commercial (trade) secrets or know-how are concerned. The burden of proof usually lies with the plaintiff but some evidence needed to

establish the infringement or its scale is controlled exclusively by the (alleged) infringer. In such cases it appears that the courts often find it difficult to assess and balance the right holder's interest in the information and the alleged infringer's interest in protecting confidential information in order to prevent abuse, in particular when the parties are competitors.

EU Member States' practice, on the one hand, shows that the protection of confidential information does not mean that access to confidential information cannot be part of provisional measures. On the other hand, access to the confidential information through provisional measures (for example by search, discovery, seizure proceedings or an injunction) may or can disclose trade secrets and it appears to be allowed only in cases where this information is truly necessary and where this information cannot be obtained by way of other (legal) means. Furthermore, a special procedure (e.g. hearing closed for the public) is usually applied when such confidential information is to be disclosed including limitation to use this information only for the purposes of the proceedings. Also, for the meaningful protection of trade secrets, their secrecy must be maintained during court proceedings so that the person lawfully in control can safely seek remedies before the court. Thus, it is very important to have specific procedures or rules to protect trade secrets before the court. Such procedures or rules may come from the code of civil procedure or court rules. At the moment based on the lack of information on this matter including clarification of the conditions as to when and how, according to the jurisprudence of the national courts, such confidential information may be disclosed would appear to be useful, the European Commission is not in a position to judge whether this situation presents an obstacle to effective enforcement of intellectual property rights[3].

Remedies

Remedies against trade secrets violations include:

- A court order to stop the person from further illegal acts (injunction)
- A court order for getting monetary compensation (damages, lost profits, unjust enrichment, etc.)
- Seizure order (to check defendant's premises, to take evidence, etc.)
- Precautionary confiscation/seizure of articles that include misused trade secrets, or products resulting from its use or misuse.

Injunctive relief

Often times, a company will be entitled to some form of injunctive relief. If the information is still a protectable secret (for example, where the other party has not publicly disclosed it), legal counsel can request an injunction and the court can order the other party to discontinue using or sharing the protected information. Injunctions may be provided for future acts of trade secret violation[4].

Article 9 of the Enforcement Directive obliges Member States to ensure that right holders are in a position to apply for an **injunction against the infringer** aimed at prohibiting the continuation of the infringement ('interlocutory', 'interim' or 'temporary' injunction). Injunctions against infringers were not new to Member States' legal systems and have been widely used in the Member States even before the adoption of the Directive. Non-compliance with an injunction is sanctioned by a fine to be paid to the plaintiff or to the court or by criminal sanctions in some cases. The reports received from

3 For more information see Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights that can be found at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0779:FIN:EN:PDF

4 For more information see Commission staff working document: Analysis of the application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights in the Member States Accompanying document to the Report from the Commission to the Council, the European Parliament and the European Social Committee on the application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights COM(2010) 779 final: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2010:1589:FIN:EN:PDF.

the Member States suggest that for most of them experiences with interlocutory injunctions have been rather positive. With some exceptions, interlocutory injunctions generally seem to be granted rather quickly by the courts and they often lead to a settlement between the parties so that the proceedings on the merits of the case can be avoided. For most stakeholders, due to the length of the judicial proceedings involving infringements of intellectual property rights and the costs of the proceedings which are rarely reflected in the damages awarded in the main proceedings, interlocutory injunctions are the **main enforcement remedy**.

Despite this generally positive assessment of the interlocutory injunctions, the information at hand suggests that the **level of evidence** required by the courts to grant an injunction differs significantly between Member States and, in general, is rather high. Moreover, it appears that some courts sometimes are reluctant to order an injunction unless an infringement has actually been proven, as opposed to granting an injunction for preventative reasons. In these cases, the 'sufficient degree of certainty' that is required by the courts is higher than what applicants are able to establish in practise. Some courts will not grant you any injunctive relief on the basis that the information is disclosed. Other courts will still grant a permanent injunction against the other party, even though the public is free to use the information, as a punishment for their wrongdoing in publicly disclosing the information.

The majority of jurisdictions that view trade secrets as a property right tend to hold that the right is only valuable as long as it remains secret and protect it for the period it remains a secret or for the period of time it would have taken the defendant to develop the same secret independently. Furthermore, in some cases, the accompanying costs can be significant, often comprising court fees, lawyers' fees and in many cases also fees of (technical) experts.

Criminal or administrative remedies

In some jurisdictions for the reasonable and balanced effective trade secret protection, criminal or administrative remedies may be more important than civil remedies. Criminal or administrative remedies may play a role in connection with the availability of civil remedies because it is often difficult to establish, or obtain evidence on, acts violating trade secrets within the framework of civil procedures in many jurisdictions.

Damages

In the most offensive situations a court can order the violator to pay exemplary damages. Damages should be recovered through either tort or contract violations.

Article 13(1) of the Enforcement Directive requires Member States to enable the competent judicial authorities to order the infringer who knowingly, or with reasonable grounds to know, engaged in an infringing activity, to pay the right holder damages appropriate to the actual prejudice suffered by him as a result of the infringement. Where the infringer acted in good faith (i.e. without reasonable ground to know), Member States have the possibility to allow the judicial authorities to order the **recovery of profits or the payment of damages**, which may be pre-established (Article 13(2)). Article 14 requires that the reasonable and proportionate legal costs and other expenses incurred by the successful party shall be borne by the unsuccessful party, unless equity does not allow it.

Since the monetary value of intellectual property may be rather difficult to measure, also due to its 'abstract' nature, practice has shown that assessing damages for infringements of intellectual property rights is often complicated. In most cases only slight adjustments of national laws governing the calculation and award of damages were needed to make Member States comply with the Directive. However, due to the relatively low number and the considerable length of the judicial proceedings, there is **not yet an established case law** on the evaluation and assessment of damages since the transposition of the Directive in the Member States. At the same time it seems that existing judgements have not been overly explicit and detailed on how awarded damages have been calculated. However, most right holders report to prefer quick provisional measures (e.g. injunctions) and not damages claims as the main enforcement remedy. The reasons for this are the high costs of the proceedings which are rarely reflected in the damages awarded and the length

of judicial proceedings involving infringements of intellectual property rights. Therefore damages awards in intellectual property cases are not requested by right holders as a matter of course.

Lost Profits

When awarding damages, it appears that all EU Member States take the **right holders' lost profits** into account. Lost profits are usually defined as profits which would have been earned by the right holder, in the absence of the infringement, or which could have been justifiably expected (excluding the infringer's profits). Nevertheless, in some Member States it seems unclear whether the price of the original product or the price of a counterfeit (which may be substantially lower in some cases) should be taken into account when assessing the right holder's lost profits. Moreover, lost profits can be difficult to prove, in particular where infringing activities undermine the value of legal sales.

Unjust Enrichment

There are several ways courts have measured unjust enrichment damages.

The **profits unlawfully made by the infringer ('unjustified enrichment')** constitute a new aspect for assessing damages in some Member States and it has been implemented into the national legislation in very different ways.

Many Member States require a right holder to prove that profits were made with or as a result of the infringing products (causal link). Infringers may sometimes make higher profits with the infringing products than the right holders with their branded goods. Right holders appear to find it very difficult to prove that they would have earned the same profits as the infringers, particularly where the infringers offer their products under conditions that significantly differ from those of the legal channels (e.g. lower prices, lower manufacturing costs, absence of related services etc.). Furthermore, in some Member States it appears that infringers' profits can only be taken into consideration once, either as a recovery of unfair profits or as damages (or part of damages), but not in a cumulative way. In other Member States the transfer of infringers' profits are awarded as an alternative, when the profits are higher than the right holder's calculated damages (e.g. the right holders' lost profits). Finally, in some Member States, in addition to damages, also the transfer of the infringer's profits may be ordered.

Royalty

The Enforcement Directive provides for two possibilities for the judicial authorities to determine the amount of the damages:

They can base the amount on the **actual prejudice** (e.g. the right holder's lost profits, the infringer's unfair profits, moral prejudice and other negative economic consequences); or they can award **lump sum damages** based on at least the (single) amount of royalties which would have been due if the infringer has requested authorisation to use the IPRs in question (e.g. if an infringer had concluded a licensing agreement with a right holder).

Further information links

Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:157:0045:0086:EN:PDF

Commission Regulation (EC) No 772/2004 of 27 April 2004 on the application of Article081(3) of the Treaty (now Article 101(3) of the TFEU) to categories of technology transfer agreements (TTBER):

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0772:EN:HTML

Commission Notice - Guidelines on the application of Article 81 of the EC Treaty (now Article 101 of the TFEU) to technology transfer agreements (Technology Transfer Guidelines):

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004XC0427%2801%29:EN:HTML

TRIPS (WTO Agreement on Trade Related Aspects of Intellectual Property Rights):

http://www.wto.org/english/tratop_e/trips_e/trips_e.htm

30 August 2003 Decision concerning implementation of paragraph 6 of the Doha Declaration:

http://www.wto.org/english/tratop_e/trips_e/implem_para6_e.htm

Hague Convention on Choice of Court Agreements:

http://www.hcch.net/index_en.php?act=conventions.text&cid=98

World Intellectual Property Organisation (WIPO) - What is a Trade Secret?

http://www.wipo.int/sme/en/ip_business/trade_secrets/trade_secrets.htm

Acknowledgments

Anna Yotova
Osterwaldstr. 143
80805 Munich
Germany
Tel: 00498933099129
Email: yotova.anna@yahoo.com

This Roadmap for Intellectual Property Protection is part of a series of guides prepared under the EU-China Project on the Protection of Intellectual Property Rights (IPR2). The series aims to provide European and Chinese companies with up-to-date information on how to protect their intellectual capital in Europe and in China. For other guides, visit www.ipr2.org or contact IPR2 (info@ipr2.org).

IPR2 is a partnership project between the EU and the PRC on the protection of intellectual property rights in China. This is done by providing technical support to, and building the capacity of the Chinese legislative, judicial and administrative authorities in administering and enforcing intellectual property rights; improving access to information for users and officials; as well as reinforcing support to right holders. IPR2 targets the reliability, efficiency and accessibility of the IP protection system, aiming at establishing a sustainable environment for effective IPR enforcement in China.

CHINA IPR SME HELPDESK

IPR2 co-operates closely with the European Union's China IPR SME Helpdesk. The China IPR SME Helpdesk is a European Union initiative, which supports European small and medium-sized enterprises (SMEs) with free information, training and first-line advice about protecting and enforcing their intellectual property rights in China. The Helpdesk offers practical information, training and workshops in Europe and China in order to assist European SMEs to make the right business decisions with regard to their China IPR matters.

If you are a European SME or SME representative body, for further information contact the European Union's China IPR SME Helpdesk:
c/o European Union Chamber of Commerce in China
Office C319, Beijing Lufthansa Center, 50 Liangmaqiao Road
Beijing 100016
T: +86 10 6462 0892
F: +86 10 6462 3206
E: enquiries@china-IPRhelpdesk.eu
www.china-IPRhelpdesk.eu

Europäisches Patentamt
European Patent Office
Office européen des brevets

The European Patent Office (EPO) is the European implementing organisation for IPR2, with the support of the EPO Member States in specific fields and the Office for the Harmonisation of the Internal Market (OHIM) on trademark and design.
www.epo.org
www.oami.europa.eu

中华人民共和国商务部
MINISTRY OF COMMERCE OF THE PEOPLE'S REPUBLIC OF CHINA

The Ministry of Commerce (MOFCOM) is the IPR2 Chinese implementing organisation.
www.mofcom.gov.cn

This publication has been produced with the assistance of the European Union.