The Legal Protection of Trade Secrets

www.ipr-helpdesk.org
ipr-helpdesk@ua.es

This document was last updated in June 2006

1. Introduction

As enterprises increasingly rely on intangible or knowledge-based assets rather than tangible or physical ones for creating and maintaining their competitiveness in the marketplace, their ability to create, deploy and strategically manage such proprietary assets is becoming a crucial factor in business success. Today's business environment has increased the importance of trade secret protection and the development and implementation of information protection practices. These must address the risks associated with a global marketplace, rapid advances in technology and telecommunications, a mobile, highly-skilled work force, and network strategic business relationships, including extensive outsourcing. Under these circumstances trade secrets are rapidly becoming, in some cases, a choice form of intellectual property protection in the information economy. Machinery and mechanisms were the brainchildren of the Industrial Age and patent law was designed to protect these. In the Information Age, trade secret protection is, in some cases, the most attractive, effective and readily available intellectual property right[1].

While the information economy has made trade secrets more important, it has also made them more likely to be stolen[2]. A more mobile workforce, the increased use of contractors and consultants, and increased infrastructure outsourcing all provide opportunities for trade secret information to leave the company's control. Information technology itself contributes to the mobility of information. Increasingly, information is stored in easily copied computer files, and internet connectivity and high-density media such as CD-ROMs make these files easy to transport. A disgruntled employee can literally walk out the door with the company in his pocket.

Adequate and effective creation, protection, use and management of trade secrets is the starting point on the road to successfully developing and managing an intellectual property strategy and integrating it into the general business strategy of an enterprise.

The purpose of this briefing paper is to provide general guidance on the law related to trade secrets. However, the details of the law vary from country to country.

If you are in doubt as to your legal rights, you should consult a specialist lawyer.

2. "Trade secrets" defined

A trade secret is commonly defined in broad terms as any information, including but not limited to technical or non technical data, a formula, pattern, compilation, programme, device, method,

www.ipr-helpdesk.org
ipr-helpdesk@ua.es

technique, drawing process, financial data, or a list of actual or potential customers or suppliers that:

1. 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
2. whose secrecy is achieved thanks to its holder's reasonable efforts.

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 include:

1. the extent to which the information is known outside the owner's business;
2. the extent to which the information is known by employees and others involved in the owner's business;
3. the extent of measures taken by the owner to guard the secrecy of the information;
4. the value of the information to the owner and to its competitors;
5. the amount of effort or money contributed by the owner to develop the information; and
6. the ease or difficulty with which the information could be properly acquired or duplicated by others.

As the list demonstrates, the *de facto* secrecy of information and the owner's continued efforts to maintain this secrecy are the key elements of a trade secret.

3. The existence of trade secrets

The subject matter of a trade secret must, as its name implies, be kept secret. Persons other than the owner may know of the secret. However, confidential disclosure to employees or others bound to secrecy will not destroy the status of the trade secret. A substantial element of secrecy must exist. Information generally known to the public or inside a particular industry is not typically afforded trade secret protection. While secrecy need not to be absolute, it must be sufficient to confer actual or potential economic advantage on one who possesses the information. Thus the requirement of secrecy is satisfied if it would be difficult or costly for others to acquire and exploit the information without resorting to some form of wrongful conduct.

Trade secret protection has been extended to a wide spectrum of information. While trade secrets are often equated with processes or product development, services can also constitute trade secrets provided they meet the abovementioned requirements. Even negative information, so-called "negative know-how", such as research options that have been explored and found worthless, can be a trade secret.

The following are a few sample categories[3] :

- data compilations, for example lists of customers (the more information a list contains, the more likely it is to qualify for trade secret protection), for example a list of customers ranked by how profitable their business is;
- designs, drawings, architectural plans, blueprints and maps;
- 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;
- costs and price information;
- information about research and development activities;
- "negative know-how", for example research revealing that a new type of drug is ineffective;
- algorithms and processes that are implemented in computer programs, and the computer programs themselves;
- manufacturing technology or repair processes and techniques;
- document tracking processes;

www.ipr-helpdesk.org
ipr-helpdesk@ua.es

- schedules, manuals, ingredients;
- prototypes;
- formulas, for example the formula of Coca-Cola (perhaps the world's most famous trade secret[4]).

A trade secret may be made up of a combination of characteristics and components, each of which by itself is in the public domain, but where the unified process, design and operation of such characteristics or components provides a competitive advantage.

Although trade secrets may elude precise definition, they are nevertheless valuable property. However, as the US Supreme Court recognized, once secrecy is lost, the property interest is destroyed forever.

4. How are trade secrets protected ?

4.1. General

Contrary to patents, trade secrets are protected without registration, trade secrets are protected without any procedural formalities. Consequently, a trade secret can be protected for an unlimited period of time. Moreover, it does not/may not cost anything (cf. Section E). For these reasons, the protection of trade secrets may appear to be particularly attractive for Small and Medium - sized Enterprises (SMEs).

Nevertheless, trade secret protection is limited. A trade secret holder is only protected from the unauthorized disclosure and use of the trade secret by others and from another person obtaining the trade secret by improper means. Indeed, it is ilicit to acquire another's trade secret if one knows or has reason to know that the trade secret has been acquired by improper means. Improper means include theft, bribery, misrepresentation, breach or induced breach of a duty to maintain secrecy, or espionage by electronic or other means. Reverse engineering or independent derivations alone are not considered improper means. Reverse engineering is the determination of someone else's trade secret information via examination and testing of publicly available information. 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.

4.2. A brief overview of trade secret protection in various countries

Depending on the legal system, the protection of trade secrets either forms part of the general concept of protection against unfair competition or is based on specific provisions or case law on the protection of confidential information. It should be pointed out that there was a noticeable movement towards increased trade secret protection in many countries of the world during the 1990's and a surprising uniformity in the treatment of trade secrets. Trade secret theft now constitutes a crime in many countries.

France: French law recognizes three types of trade secrets: manufacturing trade secrets (secrets de fabrique), know-how (savoir-faire) and confidential business information.

French law provides for penal sanctions against theft of manufacturing trade secrets (Article L621-1 Code de la Propriété Intellectuelle and Article L152-7 of the Code du Travail). Companies that are victims of manufacturing secret theft may also file a complaint before the civil courts. The same applies when the wrongful acts have not been committed by an employee but by third parties using fraudulent devices. In this case the complaint is to be filed on the

www.ipr-helpdesk.org
ipr-helpdesk@ua.es

basis of unfair competition pursuant to Article 1382 et seq of the French Civil Code. Injunctive relief, damages and third-party liability is available to the private litigant

Germany: Germany provides strong protection for trade secrets.

The new German Act against Unfair Competition (Gesetz gegen den unlauteren Wettbewerb – UWG) which came into force on 8 July, 2004, penalizes, in Chapter 4, betrayal of trade or industrial secrets (Section 17 UWG), betrayal of documents or instructions of a technical nature (Section 18 UWG), and seeking to induce another person to betrayal (Section 19 UWG).

Private litigants can also obtain injunctive relief and damages (§§ 823, 1004 Bürgerliches Gesetzbuch – BGB). There is third-party liability.

Italy: Italy provides strong protection for trade secrets. Trade secret theft is a crime (Article 513, 623 Codice Penale). The full panoply of remedies for trade secret misappropriation are available (Article 2598(3), 2600 Codice Civile). There is a third-party liability. The new Italian Code of Industrial Property ("Codice della proprietà industriale"), which consolidates all previous IP laws and which came into force on March 19, 2005, provides legal protection for corporate secret information. The Code provides that anyone who acquires or receives corporate secret information shall be bound not to use or reveal the company information and the commercial or techno-industrial experience to third parties (Article 98 and 99).

Japan: In Japan, a person whose business interests are infringed by misappropriation of trade secrets is entitled to seek an injunction, a disposal of the objects created by the act of misappropriation, and damages against the person who is infringing such business interests (Article 2, 3 and 4 the Unfair Competition Prevention Act). The amendment to the Act, which came into force on November 1, 2005, enhances criminal penalties against infringement of trade secrets. In general, this amendment newly penalizes 1) using or disclosing trade secrets outside Japan, which has been managed in Japan; 2) violating court's secrecy order outside Japan, 3) using or disclosing trade secrets by malicious retired employees; and 4) improper acquisition of trade secrets to use or disclose for the purpose of unfair competition.

Poland: Poland provides strong protection for trade secrets. The provisions of the Unfair Competition Law of April 16, 1993 as amended, cover disclosure, unfair acquisition and unfair use of trade secrets. The Law provides the injunction and other equitable remedies for the infringement of trade secrets, *inter alia*, damages and monetary relief (Article 18) and penal remedies in the form of a fine, restriction of liberty or imprisonment for up two years (Article 23).

Spain: By enacting a new Criminal Code, effective as from 24 May 1996, the imposition of fines and imprisonment for various terms (max. 5 years) is provided for a number of new crimes relating to trade secrets including the taking of data in order to discover a secret, the divulgation of stolen trade secrets by the person stealing them, breach of nondisclosure agreements and divulgation of stolen trade secrets by a third party (Article 278 and 279). Under Law on Unfair Competition (Law 3/1991 of January 10, 1991) practices of unfair competition include the infringement of industrial and commercial secrets (Article 13). The legal actions envisaged in Article 18 may be instituted against such practices.

United Kingdom: The UK provides broad and effective protection for trade secrets. Search and seizure orders may be issued to protect trade secrets and preserve evidence. There exists the full panoply of remedies for a "breach of confidence" including injunctive relief, damages and third-party liability.

USA: Many aspects of the doctrinal development of the law of trade secrets in the United States came from England. Trade secret laws are state granted rights. Nearly all states have adopted the Uniform Trade Secret Act (UTSA). The UTSA allows recovery of plaintiff's actual losses and the amount by which the defendant has unjustly benefited from misappropriation. Damages

www.ipr-helpdesk.org
ipr-helpdesk@ua.es

may include lost profits and the costs associated with repairing the damage to one's business. Exemplary (e.g. punitive) damages can be recovered in exceptional cases. Injunctions are also available. Under the Economic Espionage Act of 1996 (codified in part at 18 U.S.C. § 1831, et seq.), the theft of trade secrets is now a federal criminal offence.

5. Protection measures to be taken

The holder of a trade secret must take measures to protect and maintain its confidentiality. Typical measures to protect trade secrets include agreements with licensees and financial partners, nondisclosure agreements with employees during and after employment, warnings or notices on written materials, and physical security measures such as periodic security checks, closed-circuit monitors, and restricted access to computers and classified areas.

Taking steps to protect trade secrets from theft makes good business sense for several reasons. Preventing misappropriation from the outset is the most cost-effective way of enforcing trade secrets.

As there is no government registration in any country of the world, the cost of protecting trade secrets is largely the cost of putting in place an information security and protection policy and programme in the company in addition to the cost of monitoring, surveillance, audit and legal measures against insiders or outsiders who breach or try to breach the security system.

An enterprise-wide security and protection programme is an essential requirement for the protection of trade secrets. A basic step in developing such a policy and programme is to identify and prioritize business secrets based on their value and sensitivity in an on-going and continuous process. An effective corporate programme requires the continuous classification of new trade secrets and the de-classification of stale secrets that no longer have economic value.

When developing a company's programme, it is necessary to consider the methods that are reasonable in the light of the nature of the respective business and the trade secrets being protected, as outlined below:

5.1. Employee relationships

Employee education must be an integral part of any trade secret plan, as it is current or former employees who perpetrate the majority of trade secret infringements.

5.1.1. The situation during the employment relationship

During the term of employment, employees must be made aware of their fiduciary duty to protect confidential information and be periodically warned about situations that may result in the inadvertent loss of trade secrets. An employee may have legitimate access to an employer's trade secret, and yet treat that information carelessly. Thus there must 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.

Training and awareness are without a doubt the most cost-effective aspects of any protection programme. The keys to successful training are:

- continuity, rather than an intensive introductory course that is then not followed up; and
- accountability in order to manage its correct and effective functioning.

Apart from providing employee awareness, non-disclosure agreements are absolutely essential for protecting confidential information and facilitating the burden of proof in case of litigation (cp. below **E.2.**).

www.ipr-helpdesk.org
ipr-helpdesk@ua.es

5.1.2. The situation once the employment relationship has legally ended

Trade secret cases bring to the fore the problem of accommodating competing policies in law: the right of a businessman to be protected against unfair competition stemming from the usurpation of his trade secrets and the right of the individual to the unhampered pursuit of the occupation and livelihood for which he is best suited. There are cogent socio-economic arguments in favour of either position.

Society as a whole greatly benefits from technological improvements. Without some means of post-employment protection to ensure that valuable developments or improvements belong exclusively to the employer, businessmen could not afford to subsidize research or improve current methods.

On the other hand, any form of post-employment restriction reduces the economic mobility of employees and limits their personal freedom to pursue a preferred professional course. The employee's bargaining position is weakened because he is potentially shackled by the acquisition of alleged trade secrets; and thus, paradoxically, he is restricted by his increased expertise from advancing further in the industry in which he is most productive. It should be clearly pointed out that the *general* knowledge, skills and experience of a former employee cannot be restricted. Society as a whole suffers when competition is diminished by reducing the dissemination of ideas, processes and methods.

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.

5.2. Nondisclosure agreements

Nondisclosure agreements (also referred to as confidentiality agreements) are one of the best and most powerful tools in which confidential information is protected by trade secret owners.

Under the law of many countries, however, employees owe confidentiality to their employer even without such agreements. Thus, no contract is required to impose trade secret liability. Generally, employees are under an implied duty not to use trade secrets that they acquire during their employment in a manner adverse to the employer. However, this implied duty only arises when the employee knows or should know given the circumstances that the employer intends the information to be kept confidential. The duty to maintain confidentiality generally continues, at least for a certain period of time, even after the employee has left the job in question.

Nevertheless, a well-prepared non-disclosure contract is a must. As a matter of practice, though, employee nondisclosure agreements are a very useful part of any information protection programme because they enhance protectability in litigation[5] by giving a basis for asserting misappropriation, and they provide notice to the employees that trade secrets are considered an important asset of the company.

Nondisclosure agreements constitute, therefore, a cheap and effective technique for controlling employee misconduct, 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.

A good nondisclosure agreement is detailed and direct, and limits post-employment restrictions in time and geographical scope.

Please read also our detailed IPR-Helpdesk briefing paper on confidentiality agreements.

www.ipr-helpdesk.org
ipr-helpdesk@ua.es

5.3. Physical restrictions

A good policy provides that physical access to a trade secret document repository or to a manufacturing or research and development facility requires a security pass. A good way to block physical access to trade secret material is to separate this information from other non-proprietary information keeping it in a locked filing cabinet. Access to such information has to be limited to key personnel and should be disclosed only on a need-to-know basis.

Physical restrictions, especially regarding visitors and other outsiders, which limit access to organisation facilities and to areas containing valuable proprietary information, especially trade secrets, are essential.

5.4. Security in the electronic environment

The advent of the fully networked enterprise where intranets, extranets and the Internet are all used to gain competitive advantage has significantly increased the importance of integrating digital and information systems security measures into the security programme. Protective measures must include efforts to identify and safeguard digital intellectual assets inside the networked enterprise. However, given the speed and propagation of information, internal security measures must be supported by an external monitoring and surveillance function. Thus cybersecurity is expensive. Thus cybersecurity is expensive. For detailed information on and the installation of key and encrypted computer data accesses as well as antivirus software, so-called "red team attacks" and the protection of e-mail communication, IT professionals should be consulted.

6. Cases in which your company may benefit from trade secret protection

While a decision will have to be taken on a case-by-case basis, it is advisable to make use of trade secret protection in the following circumstances:

- when the trade secret is not protectable by any other intellectual property right;
- when the likelihood is high that the information can be kept secret for a considerable period of time. For instance, if the secret information consists of a patentable invention, trade secret protection would be appropriate if the secret can be kept confidential for over 20 years (period of protection of a patent) and if others are not likely to come up with the same invention in a legitimate way;
- when the trade secret is not considered to be of such great value to be deemed worth a patent (though a utility model may be a good alternative in countries where utility model protection exists);
- when the new information does not need to be put on the market at the time of its exploitation, e.g. when the secret relates to a manufacturing process rather than to a product, as products are more likely to be reverse engineered.

It has to be kept in mind, however, that trade secret protection is generally limited (cp.D.1.) and therefore weaker than any patent or utility model protection, and that the conditions for information to be considered a trade secret, and the scope of its protection may vary from country to country depending on the existing statutory mechanisms and case law. One should remember that courts may require very significant and possibly costly efforts to preserve secrecy. Patent and utility model protection, wherever possible, will provide much stronger protection.

7. Further links and readings

- The Identification of "Pre-existing know-how": a Strategic Issue under FP6

www.ipr-helpdesk.org
ipr-helpdesk@ua.es

- *Trends in Proprietary Information Loss* Survey of the American Society for Industrial Security/ PricewaterhouseCoopers, 1999;
- *Trends in the Proprietary Information Loss* Survey of the American Society for Industrial Security/ PricewaterhouseCoopers, 2002;
- Trade Secret Law: FAQs
- The Trade Secret Law Forum
- Further information on nondisclosure agreements
- WIPO material on Trade Secrets

---

1. For instance, it has been suggested that the most common way to protect software is through trade secret protection (see CONTU Final Report at 127).
2. A survey conducted for the American Society for Industrial Security International (ASIS) and PricewaterhouseCoopers revealed that fortune 1,000 companies lost over $ 45 billion in trade secret assets in 1999 (source: *Trends in Proprietary Information Loss Survey*).
3. To find an extensive checklist for the identification of potential trade secrets consult the Trade Secret Homepage.
4. The Coca-Cola Company goes to extreme lengths: the formula of Coca-Cola is kept locked in a bank vault that can only be opened by a resolution of the Coca-Cola Company's board of directors. Only two Coca-Cola employees ever know the formula at the same time; their identities are never disclosed to the public and they are not allowed to fly in the same airplane.
5. Courts tend to decide in favor of the trade secret holder in the presence of a contract and against the holder in the absence of a contract.