

## **Unit 6 Trade Secrets**

### **Introduction**

Although a patent application has to disclose sufficient information for an invention to be enabled (i.e. worked), there will inevitably be a considerable amount of commercial know-how which will be required to convert a patented invention into a viable commercial proposition. Thus the commercialisation of a patent through a manufacturing enterprise will typically involve: (i) pre-investment studies, including the preparation of a feasibility study and project report; (ii) engineering, including preparation of machinery specifications, plant design and factory layout; (iii) selection of equipment, plant construction, erection and installation of machinery and start-up of a plant; (iv) acquisition of manufacturing technology; and (v) technical assistance during the post-installation period, including training programmes and management assistance. However, unlike for patent rights, there is no system of registration for know-how, it will be protected only if it is regarded as confidential or if a restriction is placed upon its unauthorised communication.

In the case of employee contracts, most common law systems imply a contractual term obliging employees not to divulge information which is considered to be the property of an employer. This information will include much of the information relevant to the commercialisation of intellectual property listed above such as plant and equipment design, production methods and customer lists. This contractual term is enforceable only against an employee. To prevent a third party from wrongfully acquiring and using a person's trade secrets, the courts have fashioned rights in equity and tort against third parties.



**Example:**

The classic example of a valuable trade secret is the formula for Coca-Cola, a drink that has been available since **1866**.

The Coca-Cola Company relies on security and prosecutions to protect its invention. For example, the trade secret is kept in a bank vault in Atlanta, USA which can only be opened by a Board resolution.

Yet choosing this alternative to patenting has risks. If anyone else independently makes the same invention, they will not infringe any rights of the original inventor. Also, if others can reverse engineer the invention to obtain the secret information they could release it into the public domain, destroying the commercial advantage of the secret. In such cases patenting may be preferable.

## **2 Contractual obligations of confidence**

In intellectual property transactions, such as the possible licence of technology, sensitive information might be disclosed in order to make it possible for the other party to decide whether to enter the licence agreement or not. In these situations, usually the parties will require that a contract be entered setting out the terms of the disclosure rather than simply relying on the general law of breach of confidence.

This kind of preliminary contract will be a “confidentiality” or “non-disclosure” agreement whereby the recipient of the information undertakes not to use, disclose, reproduce or otherwise deal with the information communicated without the express authority of the person communicating it. It usually also includes a term requiring return of any hard copy documents containing the information within a certain time, or requiring return of the documents if no agreement between the parties is concluded.

Another common situation where contractual obligations of confidentiality are imposed is the employment agreement. Often, where employees will deal with sensitive and commercially valuable information, the terms of the disclosure and the employees’ use of the information are set out in the contract appointing the employee.

## **3. US Trade Secret Law**

First, there is the US tortious cause of action called “misappropriation of a trade secret”. This requires that the information is a “trade secret”, e.g. a secret used in a business, that is actually secret (not known by the general public) and which gives a competitive advantage to the person with knowledge of it. It also requires that the trade secret was “misappropriated”, for example acquired improperly, or in breach of confidence or with knowledge of certain factors.



The action in tort for misappropriation of a trade secret has been codified in many US States into legislation. The trade secret legislation in these States is modelled on the *Uniform Trade Secrets Act*, although there are differences in the drafting of the State legislation. This legislation provides for injunctions and damages for misappropriation of trade secrets.

Various State legislation has also enacted separate provisions making unauthorised disclosure of trade secrets a crime (eg. the Californian Penal Code §499c).

There is also relevant federal legislation. Intentional theft of trade secrets that are “related to or included in a product that is produced for or placed in interstate or foreign commerce” may breach the *Economic Espionage Act of 1996* 18 USC §1831-§1839. Under this legislation, there are significant fines (eg. companies up to US\$5 million), and the possibility of prison sentences for theft of trade secrets.

## **2. Protection under the TRIPS Agreement (Art. 39)**

### **(a) Introduction**

The protection which is conferred upon certain categories of confidential information by Art.39, represents the first time that such information has been specifically protected in an international intellectual property convention beyond the general obligation in Art.10*bis* of the Paris Convention which provides for the assurance to nationals of the Paris Union of ‘effective protection against unfair competition’. The scheme of Article 39 is to provide in paragraph 1 for the general protection of confidential information described in paragraph 2 and in paragraph 4 for the protection of undisclosed test data submitted to government approval authorities.

### **(b) Confidential Information and Unfair Competition**

Article 39.1 provides that ‘In the course of ensuring effective protection against unfair competition as provided in Article 10*bis* of the Paris Convention (1967), Members shall protect undisclosed information’ of the sort which is described in paragraphs 2 and 3 of Art.39. Paragraph 2 describes the general category of confidential information which is protected in common law countries through judge-made law, rather than through statute. Article 10*bis* contains no reference to the protection of confidential information as an aspect of unfair competition. Article 10*bis*(2) defines as an act of unfair competition ‘any act of competition contrary to honest practices in industrial or commercial matters’. Article 10*bis*(3) lists three particular practices which are to be prohibited. The first two concern unfair acts or allegations directed against a competitor and the third category concerns the misleading of the public about aspects of goods to be supplied to them. Article 10*bis* is a novel context in which to deal with confidential information since, at least in its common law context, there is no requirement the parties to an action be involved in a competitive relationship and there is no hint in the article itself, or in the official commentary on Art.10*bis* that it applied to confidential information.



Most common law jurisdictions have been hostile to the development of a general remedy in respect of unfair competition. However, certain categories of unfair competition, such as passing off, injurious falsehood and deceit have been developed to protect a trader's commercial reputation. The action for breach of confidence has never been considered to be a species of unfair competition, but this may be explicable as a means of using the Paris Convention to incorporate the action within the TRIPS Agreement over the objection of those countries which argued that it was outside the scope of traditional intellectual property laws.

Some of the flavour of Art.10*bis* is imported into para.2 of Art.39 of the TRIPS Agreement through conferring upon 'natural and legal persons' the right to prevent the disclosure of confidential information which is 'lawfully within their control' and 'without their consent in a manner contrary to honest commercial practices'. A footnote to the paragraph defines the phrase 'a manner contrary to honest commercial practices' to mean 'at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew or were grossly negligent in failing to know, that such practices were involved in the acquisition'.

### **(c) Protecting Confidential Proprietary Information**

Article 39.2 provides for the protection of information which (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 or 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.

#### *Confidentiality*

As a general rule, to be protected, information must be confidential and not in the public domain, for example by being published in a patent specification. In deciding, for example, whether an employee could rely upon his acquired knowledge in the service of an employer, the US *First Restatement of Torts*, applies the following criteria, some of which are listed in Art.39.2:

- (1) The extent to which the information is known outside of [the employer's] business;
- (2) the extent to which it is known by employees and others involved in his business;
- (3) the extent of measures taken by him to guard the secrecy of the information;
- (4) the value of the information to him and his competitors;
- (5) the amount of effort or money expended by him in developing the information;
- (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.

Article 39.2 conceives of the possibility that information may be considered to be confidential if elements of it are in the public domain, but the know-how or method of combining or aggregating those elements is confidential.



### *Obligation of confidence*

To succeed in an action for breach of confidence, not only must the relevant information not be in the public domain, but it must be communicated in circumstances which import an obligation of confidence. In *Coco v. A.N. Clark (Engineering) Ltd* [1969] RPC 41, the leading English decision, Megarry J. enunciated an objective test in determining whether the obligation of confidence applied to the communication of information, explaining that ‘if the circumstances are such that any reasonable man standing in the shoes of the recipient of the information would have realised that upon reasonable grounds the information was being given in confidence, then this should suffice to impose upon him the equitable obligation of confidence’.

The obligation of confidence binds not only the direct recipients of confidential information, but also third parties who receive that information and who are aware that it has been disclosed to them in breach of confidence. This will usually be the situation in trade secrets cases where a former employee carries those secrets to his new employer.

#### **(d) Categories of Protected Information**

There are very few limits to the sorts of undisclosed information which have been protected in the action for breach of confidence. However, the trade-related context of Art.39 may provide a limit to the wholesale importation of breach of confidence principles. Article 39.1 suggests that the provision is an amplification of Art.10*bis* of the Paris Convention, which is concerned with unfair competition. Another limiting factor is the location of Art.39 within an agreement concerned with intellectual property.

Undisclosed information is an invariable adjunct to most intellectual property rights. For example, patent protection is conferred in exchange for the disclosure of sufficient information in a patent application to permit the invention, which is the subject of the application, to be worked. Inevitably, to protect its competitive advantage, the applicant will withhold information concerning the ways in which an invention will be effectively commercialised. This information, or know how, will include: plant design and set-up, training, marketing plans, customer lists, and accounting and survey methods. Article 39 recognises the necessity to protect these categories of undisclosed information to permit the effective commercialization of patents rights, among others.

Similarly, a protected trademark is of limited commercial utility without an associated scheme for the advertising, licensing, franchising and marketing of goods or services under that mark. Ensuring control of the quality of licensed goods will usually entail the application of trade secrets.

Where undisclosed information has been recorded, some limited protection may be obtained under copyright law. Where, however, the recordal is only of an idea, copyright protection will not avail, as that jurisdiction protects only the way in which ideas are



expressed. The jurisdiction in confidence has been the principal means by which the commercial exploitation of undisclosed ideas may be restrained.

**(e) Undisclosed Test Data**

As is mentioned in the introduction above the TRIPS Agreement negotiators were anxious to preserve the confidentiality of test data submitted to government approval agencies. Given the long approvals process, particular for pharmaceutical products, the opportunities for wrongful appropriation of such data by competitors was self evident. This concern is accommodated by Art.39.3 which provides that

Members, when requiring , as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort, shall protect such data against unfair commercial use. In addition, Members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use.

It should be noted that Art.39.3 contains three limitations. First, it applies only to pharmaceutical products and chemical agricultural products; secondly, the protection is extended only against unfair commercial use; and, thirdly, the government authority is exempted from the requirement of confidentiality in the public interest. Thus it has been held that a government accrediting agency may use the confidential test data of an applicant when considering applications by other applicants in respect of similar products.

