"In Confidence" – Putting in Place a Trade Secret Protection Program

Training of the Trainers Program on Effective Intellectual Property Asset Management by Small and Medium Sized Enterprises (SMEs)

WIPO & IPOM, Mongolia

Ulaanbaatar, October 8 to 10, 2013

Susanna H.S. LEONG
Associate Professor & Vice Dean
NUS Business School, National University of Singapore

Protection of Trade Secrets - TRIPS

- In TRIPS, the obligation of member states to provide protection for confidential or undisclosed information is found in article 39 which provides:
  - (1) 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 in accordance with paragraph 2 and data submitted to governments or governmental agencies in accordance with paragraph 3.
  - (2) 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. [emphasis added]

Protection of Confidential Information under Common Law

- At common law, a plaintiff who alleges a breach of confidence must establish all of the following:
- (a) the information must have the necessary *quality of confidence* about it;
- (b) the information must have been imparted in circumstances importing an *obligation of confidence*; and
- (c) there must have been *an unauthorised use* of that information to the *detriment* of the party communicating it.

TRIPS vs. Common Law

- Confidential or undisclosed information is thus protected under the auspices of unfair competition laws when dealt with in a manner contrary to honest commercial practices.
- Footnote 10 to article 39(2) of TRIPS states that for the purposes of this provision, "a manner contrary to honest commercial practices" shall include practices such as breach of contract, breach of confidence and inducement to breach, and also 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.
- The scope of protection for confidential or undisclosed information under article 39 of TRIPS is more restrictive than common law as it covers only secrets that have commercial value.

The information must have the necessary quality of confidence

- It is generally accepted that to qualify for protection under the law of confidence, the information need not be new or contain any inventive ideas unlike the requirement under patent law.
- Furthermore, the mere simplicity of an idea or information will not detract from its confidential nature.
- The common law of confidence does not limit its protection to only one particular type of information such as trade or commercial secrets nor does it confine the application of the law to information with commercial value by virtue of it being secret.
- Roskill J in *Cranleigh Precision Engineering Ltd v Bryant* [1965] 1 WLR 1293 rejected the contention that the confidential information concerned did not possess the quality of confidence solely because of its simplicity.
- Also, Megarry J in *Coco v A N Clark (Engineers) Ltd* [1968] FSR 415 at 421 concurred with Roskill J's view and said "the simpler an idea, the more likely it is to need protection".
- In Singapore, this view has also been endorsed by Justice Lai Siu Chiu in *QB Net Co Ltd v Earnson Management (S) Pte Ltd* [2007] 1 SLR(R) 1 at [79].

The information must have the necessary quality of confidence

- Any kind of information, factual or fictional, commercial or governmental and even private or personal, which the law considers as important and of value can qualify as confidential information.
- Confidential information may be broadly classified into the following categories:
  - (a) commercial, technical/industrial and other analogous secrets;
  - (b) personal or private secrets; and
  - (c) Government secrets.

Commercial, technical/industrial and other analogous secrets

- Information such as secret recipes, processes, formulae, engineering drawings, customer lists and business strategies fall within this category. Commercial and technical/industrial secrets is subject-matter which is often considered to possess pecuniary value and constitutes valuable business assets.
- Therefore, they are considered by most to be appropriately within the domain of intellectual or industrial property and warrant protection.
- Examples of information given protection include:
  - (a) a process for making swimming pools (*Cranleigh Engineering v Byrant*);
  - (b) designs of a moped engine (*Coco v A N Clark (Engineers) Ltd*);
  - (c) an industrial process for cleaning ships (*Underwater Welders & Repairers Ltd v Street & Longthorne*);
  - (d) the genetic information needed to reproduce a variety of nectarines imprinted in the twig wood or scion wood of the nectarine tree itself (*Franklin v Giddins*);
  - (e) books of account and other internal financial and commercially-sensitive information of a business (*Tipping v Clarke*); and
  - (f) information regarding the financial affairs, management procedures and trading practices of a company (*Vestwin v Obegi*).

What form must the information be in?

- Confidential information need not be in a material form or take any particular material form.
- It can be written, oral, or even embodied in an artistic work or a physical object.
- In *Fraser v Thames Television*, the idea of a television show was orally described to a producer and the court had no difficulty finding it confidential. In *Douglas v Hello! Ltd* and *Prince Albert v Strange*, confidential information was found to exist in artistic works such as photographs and etchings respectively.
- In *Franklin v Giddins*, when the defendant cut a piece of wood from the plaintiff's tree in which the plaintiff had been cross-breeding a particular species of nectarines, the court ruled that the defendant had taken away confidential information of the genetic make-up of the tree.
- In *Ackroyd v Islington Plastics*, the plaintiff provided tools to the defendant to produce swizzle sticks and the court found that any information that the defendant gained from using the tool provided by the plaintiff was confidential information.

Is originality, novelty or ingenuity of information a pre-requisite for protection?

- In essence, the information need not be new or contain any inventive idea to qualify for protection under the law of confidence.
- More importantly, for the purposes of an action in breach of confidence, the information must not be found in the public domain and not be required to be disclosed in the public interest.

Confidentiality and the public domain

- In order for the information concerned to possess the necessary quality of confidence, the most important criterion is that it must not be common knowledge.
- This means that the information must be confidential and "it must not be something which is public property or public knowledge".
- Two important factors help determine whether the information is in the public domain:
- (a) degree of exposure or publication of the information; and
- (b) accessibility of the public to the information.

Confidentiality and the public domain

- It is difficult to set out specific guidelines as to the extent or degree of publication necessary to render the information part of the public domain and thus no longer confidential.
- Although the number of persons who have knowledge of the information is a relevant consideration, it is not conclusive.
- If the information has been disclosed to a limited number of people, it could be said that the information has not entered the public domain in the sense that it is not widely known and therefore confidentiality of the information is preserved.
- Indeed, some authorities suggest that even though secrecy may be imperfect in relation to a communication given in confidence, that communication may still be protected by the principles of confidentiality.
- Therefore, information is still considered confidential even though it has been disclosed to some people, as long as it is *relatively* secret.
- In *Abernethy v Hutchinson* (1825) 1 H & Tw 28, a lecturer who gave a medical lecture to a group of students was still able to succeed in an action for breach of confidence to restrain a student from publishing parts of his lecture. The fact that the lecture was made to the entire class of students did not jeopardise the plaintiff's case.

Confidentiality and the public domain

- If, on the other hand, the information is generally known to the public at large, the conclusion would be that the information is now in the public domain and confidentiality of the information lost.
- For example, once a patent had been granted covering the information claimed to be confidential, the information was disclosed to the public at large and all confidentiality attached to it destroyed.
- However, even when information is disclosed to a large number of persons, a case can still be made that it remains confidential and has not entered the public domain.
- An important consideration is whether the persons who have knowledge of the confidential information are under any obligation in law not to further disclose or use the information without consent.
- If they are, the information is not common knowledge and continues to have the necessary quality of confidence about it.
- As we have seen in the foregoing discussion, whether information has become so widely known that it is in the public domain is really a question of fact to be decided on the circumstances in individual cases.

Confidentiality and the public domain

- Another helpful indicator is the accessibility of the information by the public.
- Geographical location can sometimes play a role.
- Impact of the Internet.
- Confidential information may even be generated by compiling or incorporating materials or information in the public domain that is common knowledge.
- In this regard, some courts have required the added element that there must be some degree of originality or ingenuity in the information before it can be considered confidential.
- Old information which is in the public domain can reacquire confidentiality merely through the passage of time.

Obligation of Confidence

- The defendant is under an obligation in law to keep confidential the information communicated to him by the plaintiff.
- If the law does not consider that the defendant is under such a duty or obligation, there can be no breach.

When does an obligation or duty of confidence arise?

- Particular relationships
- Examples of relationships include that of a doctor and a patient; a priest and a penitent; a solicitor and a client; a banker and a customer, a husband and wife and very close friends who freely discuss matters of a personal and private nature.

When does an obligation or duty of confidence arise?

- Express contractual term
- A typical example is the non-disclosure agreement frequently entered into by parties in the initial negotiation process with investors to develop and commercialise new products or inventions.
- A breach of confidence by the confidant in such cases will constitute a breach of contract, resulting in contractual remedies for the innocent party.

When does an obligation or duty of confidence arise?

- Equity
- Even in the absence of particular relationships, equity may impose an obligation of confidentiality.
- Where the information was communicated and accepted expressly in confidence, the law will impose a duty of confidence on the person who has received the information. However, in the absence of an express statement that the information is confidential, courts need to determine under what circumstances a recipient of information owes a duty of confidence to the confider.
- Reasonable man's test

When does an obligation or duty of confidence arise?

- Disclosures during negotiations with a view to commercial exploitation
  - *Seager v Copydex*
  - *Carflow Products v Linwood*
  - *Flamelite v Lam Heng Chung*
- Disclosures of information for a limited purpose
  - *Pollard v Photographic Co*
  - *Ackroyd v Islington Plastics*
  - *Schering Chemicals Ltd v Falkman Ltd*

Can employees take confidential information away from employer post employment?

- In regulating the relationship between employer and employee, different interests are at stake and they often conflict with one another.
- On one side is the employer's private interest in maintaining confidentiality of information whilst on the other side is the public interest in freedom of employment and encouraging competition.

Can employees take confidential information away from employer post employment?

- A possible reconciliation of these conflicting interests is for the law to treat employees currently in service differently from ex-employees.
- Much more is expected of the employee who is in current service and the balance of interests is tilted in favour of protecting the employer's private interest.
- However, post termination of employment, the balance of interest shifts in favour of the ex-employee to uphold freedom of trade and competition.

During contract of employment

- During the contract of employment, an employee is first and foremost bound by express terms found in his contract of employment which may spell out his obligations of fidelity and confidentiality. Apart from express terms, an employee also owes an implied duty of fidelity:
  - (a) not to compete with his employer; and
  - (b) not to disclose or use to the detriment of his employer confidential information which has come into his possession or knowledge as a result of his employment.
- An unauthorised disclosure of confidential information by an employee to third parties during his contract of employment is a breach of both the duty of fidelity and the duty of confidentiality.
- Employee suggestion scheme – implications?

After termination of contract of employment

- Post termination of employment, an ex-employee may be constrained by:
  - (a) express contractual covenants that continue to apply after termination, in particular restraint of trade clauses; and
  - (b) an implied equitable obligation of confidence.

Restraint of trade clauses - Illustrative Cases

- Moat v Mills
- The defendant was employed in a paper tissue company. When he left the company, he signed a severance agreement and was given a sum of money for his resignation.
- In the severance agreement, he agreed not to work in a company within the paper tissue industry for a period of one year.
- Thereafter, the defendant joined the plaintiff's competitor as managing director.
- The plaintiff sought an injunction.
- The English Court of Appeal held that the severance agreement was in restraint of trade because it was not limited geographically or limited in the scope of the activities it sought to restrain.
- The court refused to construe the clause so as to render it valid.

An implied equitable obligation of confidence – Distinction between "know how" and trade secrets

- As to the kind of information which the court will restrain an ex-employee from disclosing or using post contract of employment, it is clear that only information that is considered by the courts as *trade secrets or its equivalents* is protected.
- Trade secrets obtained by the employee in the course of employment must be distinguished from the employee's general stock of knowledge and skill.
- There can be no restraint by the employer in respect of the ex-employee's practice of his general stock of knowledge, skill and talent, even if they are acquired by the ex-employee in the course of his or her employment.

What constitutes a trade secret?

- Factors which courts take into consideration:
  - (a) *The nature of the employment* – where the employee habitually handles confidential information, a higher obligation of confidentiality may be imposed.
  - (b) *The nature of the information itself* – in this regard, the information concerned must be a trade secret or material which, while not properly to be described as a trade secret as such, is having regard to all the various circumstances, "of such a highly confidential nature as to require the same protection as a trade secret".
  - (c) *Whether the employer impressed on the employee the confidentiality of the information* – in order to prevent the use or disclosure of the information in question, it was insufficient for the employer to merely tell the employee that the information was confidential. The employer's attitude towards the information itself had to be considered as well.
  - (d) *Whether the relevant information can be easily isolated from other information which the employee is free to disclose* – where the information alleged to be confidential is 'part of a package' and the remainder of the package is not confidential, this factor, although not conclusive in itself, can shed light on whether the information in question is truly a trade secret.

Unauthorised use or disclosure of information

- Unauthorised use refers to any disclosure or use which contravenes the limited purpose for which the information was revealed.
- In an action for breach of confidence, the plaintiff must prove that the defendant made use of the information which came from the plaintiff and not from any other source such as reverse engineering, and that the use of the information was without the express or implied consent of the plaintiff.

From a Firm's Perspective: To Patent or Not to Patent?

- Secrecy v Disclosure
- (1) the trade secret believed by its owner to constitute a validly patentable invention;
- (2) the trade secret known to its owner not be so patentable; and
- (3) the trade secret whose valid patentability is considered dubious.

From a Firm's Perspective: To Patent or Not to Patent?

- With regard to (1), trade secret law provides far weaker protection in many respects compared to patent law.
- Trade secret law offers no protection if the trade secret is discovered by fair and honest means, e.g. independent creation or reverse engineering.
- Patent law on the other hand gives protection against the world forbidding any use of the invention for whatever purpose for a significant length of time.
- Also, trade secret holder runs the risk of his secret being passed on to his competitors, by theft or by breach of confidential relationship, in ways not easily proven or discovered.
- Therefore, the possibility of an inventor who knows or believes that his invention meets the stringent criteria of the patent office will however rely on trade secret law and forfeit any right of patent protection is very remote.

From a Firm's Perspective: To Patent or Not to Patent?

- With regard to (2), since trade secret is not patentable because it does not meet the requirements of patentability, the likely cause of action of the inventor is to keep it secret.
- With regard to (3), no clear cause of action – dependent on the nature of the trade secret; involves a cost-benefit analysis. Example Coca-Cola Inc.

From a Firm's Perspective: To Patent or Not to Patent?

- Difficulties faced by an inventor who seeks to maintain confidentiality of the information embodied in an invention whilst simultaneously filing a patent application for the invention.
- More often than not, inventors and business people do not fully appreciate the consequences of a full and sufficient disclosure of the invention when filing for a patent and its impact on maintaining the confidentiality of the information embodied in the patent specification.

From a Firm's Perspective: To Patent or Not to Patent?

- Confidential information will remain protected as long as it remains confidential.
- There is technically no limit on the duration of protection for confidential information, quite unlike patents which enjoy only a limited period of protection.
- Theoretically, in the case of commercial or trade secrets, the duration for which a business person may maintain market dominance for a particular product could be much longer if he chooses to keep it a secret as opposed to filing a patent for it.
- The obvious drawback is, of course, the potential risk of disclosure associated with the sale or commercialisation of the product.
- If the public is able to discover the secret information embodied in a product by reverse engineering once it is put on the market, the secret information embodied therein is no longer a secret and cannot be protected anymore.

From a Firm's Perspective: To Patent or Not to Patent?

- The ease with which information may be distributed and shared over the internet today can certainly hasten the process of confidential information shedding its cloak of confidentiality.
- Whether businesses should choose to protect their confidential information through patents for a limited period of 20 years or to rely on the common law of confidence which may provide protection for an indefinite period of time as long as the information remains a secret is, at the end of the day, a decision the board of directors has to make taking into consideration the nature of the confidential information concerned.

Thank You!

Questions?