METS IGNITED IP MASTERCLASS

DENNEMEYER TRADE SECRETS BLOG

The Masterclass presenters have prepared articles relating to the protection of Trade Secrets, and these have been published on Dennemeyer's website.

The articles are:

- "Trade Secrets – The Need to be Systematic "
- "Trade Secret or Patent – How do we decide? "
- "How to craft an effective CDA - the essentials"

Further articles on IP and its management can be found on: www.dennemeyer.com

Trade secrets – the need to be systematic

Dr. Dallas Wilkinson, John Walker / August 13, 2019

The term "trade secret" is invariably included in any definition of "Intellectual Property." However, while the majority of IP types are subject to strict rules, guidelines and timeframes due to the requirement of registration (e.g. patents, designs and trademarks), trade secrets do not require such formalities. Or do they?

Most people are aware of the Coca-Cola story – possibly the world's most famous trade secret - whose recipe has been kept secret since 1886. This has been the result of a carefully considered protection and "disclosure" strategy whereby access to the secret is strictly limited and restricted. While such a recipe can be a trade secret, virtually anything that adds value to a business can be regarded as a trade secret, and can include any method, formula, device, process or any information (technical or business, e.g., a list of suppliers) that gives its owner a competitive advantage. Even the results of failed R & D programs might be considered as a trade secret – providing a springboard for new research directions. Further, these trade secrets may be stored in a variety of ways ranging from traditional paper copies (e.g. reports and manuals) to computer and other digital forms, or even retained in the mind of employees without any documentation.

Before embarking on a trade secret protection strategy, the owners must first ask several key questions:

- Do they know the information is actually a secret (confidential)?
- Do they know they have them?
- Who controls the secret information ?
- Where is the information held, how and in what form?
- Who has or has had access (both internally and externally)?
- Who needs to know the trade secret in its entirety or can the secret be broken up, so only few people know the entire secret? This is an effective control measure.

Additional questions include:

- What value does the owner place on these secrets?
- Is this value understood widely or only by a select group of individuals?
- Is the value realized in the short term or long term?

Once this analysis has been undertaken, consideration is required as to how such secrets might be disclosed – inadvertently or deliberately. Disclosure might be through publication, at a seminar, during meetings, informal conversations, accidental or inadvertent disclosure, as well as theft. On occasion, a small amount of information may be released in order to create value, build up a brand or support other commercial reasons. Except for theft, all of these disclosure mechanisms can be controlled or minimized by effective policies, procedures and systems.

Having identified the nature of the secrets and how they might be disclosed, the next consideration is to **identify the risks in the business or technical environment** where inappropriate disclosure may occur. In simple terms, these sources of risk might be external or internal. External sources include competitors (naturally) as well as any entity who the owner may have some (potential or existing) collaboration or business relationship with – licensees, JV partners, customers, suppliers, toll manufacturers, consultants, etc. The most pertinent source of internal risk are the employees themselves and the owner's lack of confidentiality policies or processes.

Typical requirements of a Confidential Disclosure Agreements include defining the information being disclosed, the purpose of such disclosure, the duration of the secrecy obligation and how the information is disclosed.

As already indicated, trade secrets are not registrable but are the subject of common law. Although the foregoing has set out several questions a trade secret owner must consider, ultimately the owner must be in a position to take legal action for the misappropriation or misuse of trade secrets, particularly where there has been a considerable commercial loss – somewhat analogous to patent infringement. To enhance the likelihood of a successful legal outcome, the courts will need to assess whether the secret was, in fact, something the public or industry did not know or could easily find out, whether the secret provided the owner with a competitive advantage, and importantly whether there had been reasonable efforts by the owner to maintain its secrecy. Some of these efforts or approaches, as well as their practical considerations, are identified below.

Like any business process, it is often advisable to conduct a risk assessment on the trade secret and understand the elimination and mitigation controls an organization can put in place to manage the secret. Confidential Disclosure Agreements (CDA), often called Non – Disclosure or Secrecy Agreements (NDA), are a common protection technique. Typical requirements of a CDA include defining the information being disclosed, the purpose of such disclosure, the duration of the secrecy obligation and how the information is disclosed (e.g. written, verbal etc). Of course, all of these specifics relate back to the initial questions referred to earlier – identifying the secret, how the secret might be disclosed and the sources of risk. In addition to the use of a suitably crafted CDA to reflect the business environment and objectives, the owner has other techniques at its disposal to mitigate or minimize

disclosure risks. These can include marking materials as "Confidential", securing the documentation, limiting copies, developing physical and other security measures (e.g. passwords) or limiting access to only segments of the secret. For example, the "Coca-Cola technique" includes maintaining registers of disclosures, appropriate employment agreements, as well as clear and concise communication of secrecy policies and educating employees of the owner's policies and procedures.

The protection of a trade secret requires different considerations from IP protection through a registration system such as patents. To obtain a patent and thereby protection, the applicant must comply with stated rules, whether such rules relate to patentability criteria, meeting timelines, disclosing the technology to the public or paying fees. Whether this patent protection is at a local or international level, these rules are clearly defined and set by a national or international government agency. It is with this background that IP databases have developed to systemize these externally imposed rules and requirements. Nonetheless, successful trade secret protection requires the consideration of a wide range of parameters – albeit less rigid than patents, as well as a diverse set of processes and policies. When these parameters, processes and policies are assessed, a more formalized and systematic approach to trade secret protection can be developed.

The Dennemeyer Group provides a wide range of IP protection and management services to clients throughout the world. As a result, Dennemeyer is particularly well placed to advise business owners on strategies for the overall protection of their intellectual assets, including the development and implementation of trade secret protection strategies consistent with protection through established IP registration regimes.

Trade secret or patent protection – how do we decide?

Dr. Dallas Wilkinson, John Walker / January 21, 2020

In our recent article on trade secrets, we indicated that virtually anything that adds value to a business could be regarded as a trade secret, and this may include any method, formula, device, process or information (technical or business, e.g., a list of suppliers) that gives the owner a competitive advantage. In this article, we focus on the factors to consider when determining how to protect technological innovation, and particularly whether to patent or keep as a trade secret.

In our first piece article of the series, we also mentioned possibly the world's most famous trade secret - whose recipe or "chemical composition" has been kept secret since the 1880s. This "product and method" fades into insignificance compared to the "secret" method of making Chartreuse liqueur. This was first "invented" in 1605 and has been in commercial production since 1737. So, it can be done provided protection strategies are well-planned and implemented. When it comes to technical innovations, we start by considering patentability criteria. Most jurisdictions have five main requirements for patentability. These are:

1. The patentable subject matter,
2. Novelty,

3. Utility,
4. Whether the innovation involves an inventive step (the obviousness test), and finally
5. Whether the innovation has had prior commercial use (e.g., A key test: has the product been sold already?).

Because trade secrets have no specified criteria, they also can be considered to fit these patentability requirements – except, unlike patents, there is no Patent Office examination process to test them. The last criterion is always an area where organizational awareness is frequently lacking and can have a detrimental impact. Often innovative companies may prevent themselves (inadvertently or otherwise) from obtaining patent protection by commercially using (such as selling) their innovation before filing a patent application. In such circumstances, the only protection remaining is a trade secret, provided that the company can retain that status and manage the secret- now and in the future! We strongly recommend the training of commercial and technology team members to increase awareness of these criteria to manage this commercialization risk.

Given the background outlined above, we can now look at several questions that should be raised when making a conscious decision.

To patent or to keep secret?

The first issue is the **subject matter**. All jurisdictions have limitations on the patentable subject matter, whereas a trade secret can relate to anything, provided the owner considers the secret offers some competitive advantage and is valuable. **Patentability criteria** have been mentioned above, and again there is no test for a trade secret to satisfy, only this subjective competitive advantage assessment. **Claims** made by the patentee ultimately determine patent protection, and again there is no requirement for a trade secret to satisfy particular drafting needs. An underlying requirement and cornerstone of the patent system is for the patentee to **disclose the invention** in the patent application, which, of course, is the exact opposite of trade secret protection. One approach to managing this aspect is to prepare the "secret" as though you were going to file a patent application – this will help the understanding of the potential uniqueness / differentiation (and thus value) of the secret.

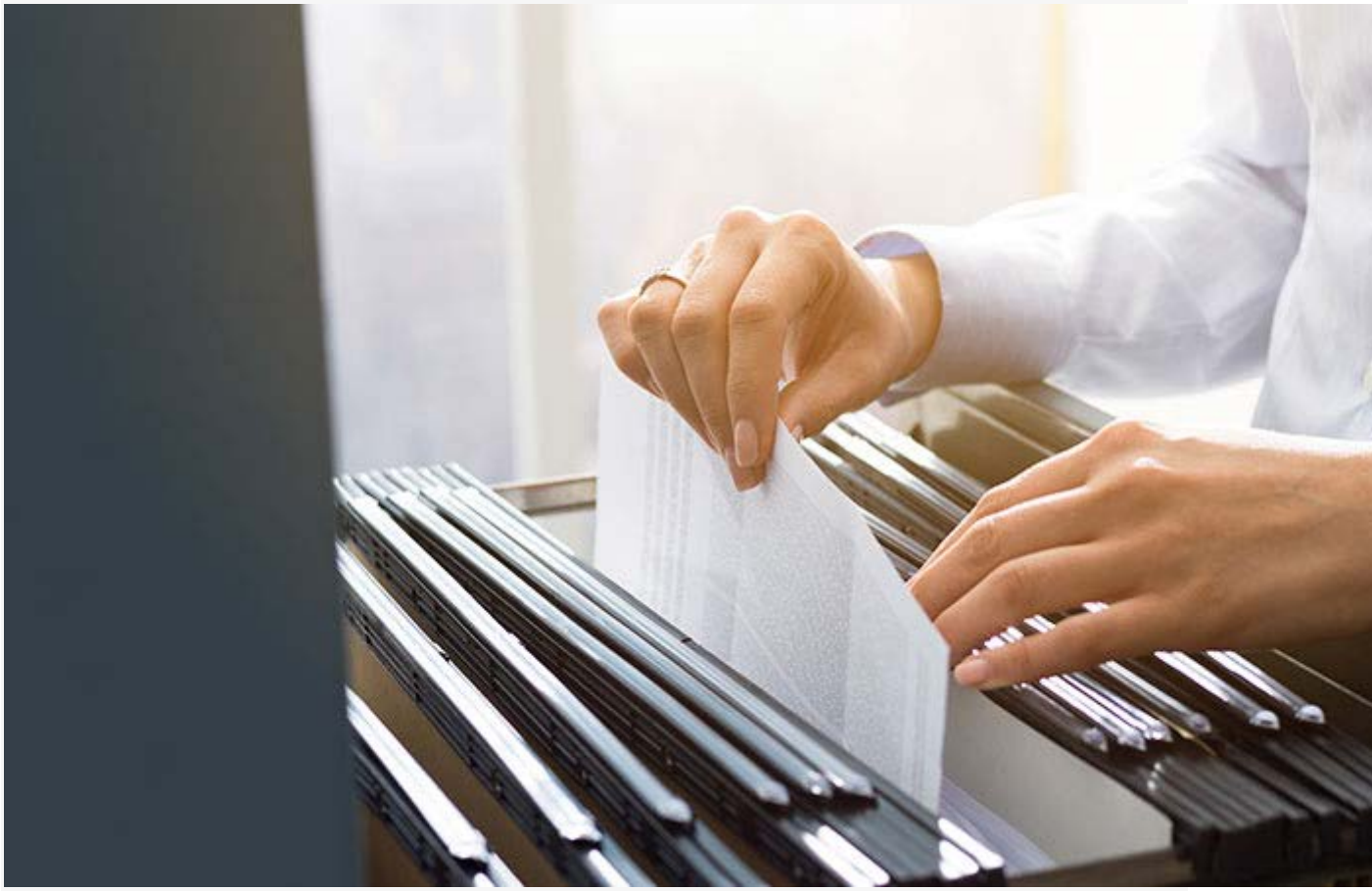
One approach to deciding whether to patent an invention or keep it a secret is to prepare as though you were going to file a patent application– this will help the understanding of the potential uniqueness / differentiation of the secret.

As indicated by the earlier examples, the **duration** of trade secret protection is potentially infinite, assuming it can be kept secret. You can compare this with the 20 years virtually universal period of protection for patents. The question of duration will often depend on the type of invention. For example, a software type development may only have a product life cycle of five years and this would tend to favor the trade secret option. On the surface, the **cost of protection** would seem to support seeking trade secret protection. Typically a reasonably broad geographic patent filing, examination and grant strategy might cost over USD200,000 and the costs of policing possible infringers can raise this significantly. However, to protect a trade secret against unauthorized use may not be as simple as a "one size fits all" non-disclosure agreement. Consideration of the best protection mechanism needs to take into account the nature of the trade secret, which may include:

- How the technology might be copied / stolen
- Who might copy / steal the technology
- Can the technology be easily reverse engineered by someone skilled in this technology and
- How the technology may develop in the future (e.g., future new generations of the technology).

These considerations might not simply involve just legal protection (such as agreements), but also physical security means. The various issues to examine when preparing confidential disclosure agreements and when to use them will be discussed in a future article in this series.

The patent claims referred to earlier are the basis upon which the patentee is protected. Even if an infringing party independently developed the patented invention, this will not form a defense for patent infringement. This issue, of course, is not applicable for trade secrets. It is worth stressing that **independent development** does not offer the trade secret owner any protection, nor does **reverse engineering**. The owner of a trade secret is powerless to prevent a competitor who chooses to reproduce a product or copy a process that is protected by a trade secret, assuming there has been no theft or illegal activity involved. The concept of reverse engineering can be a critical one in the decision process for chemical compositions as it is often the "secret" production method (such as a unique combination of chemistry and process parameters including temperature, pressure, time, etc.) that really characterizes the invention and provides the commercial advantage. In short, trade secret protection is only useful against **"unfair"**or**"illegal"**users, whereas enforcing patent protection is based on clearly defined principles of claim infringement, irrespective of how such infringement came about.



Trade secret is potentially infinite, but the question of duration depend on the type of invention. For example, a software type development may only have a product life cycle of five years and this would tend to favor the trade secret option.

Both protection approaches involve **risk**. The patent system centers on invention disclosure, and while examination procedures in major jurisdictions are very thorough, it is possible, for example, to miss relevant prior art during the examination process. This has the potential to lead to **patent invalidity.** The alternative protection method, a trade secret, is not risk-free either. While the owner may believe they have taken all necessary steps to protect the secret, the risk of disclosure (either inadvertent or deliberate) is always present. Again, independent development by a third party lurks as a potential reason not to protect as a trade secret. In some jurisdictions such as the U.S., the law is becoming stronger to protect the trade secret holder, but there is considerable variation throughout the world.

Commercially exploit the invention to external parties

The foregoing discussion centers largely around protecting an invention for internal commercial use and application. However, where the owner intends to commercially exploit and market the invention to external parties (for example, through licensing), other factors in this protection decision emerge. The licensing of patented technology is easier to implement. The technology being licensed is precisely defined and license terms relating to patent validity and infringement in a license agreement can be clearly set out. Trade secret licensing (and sometimes "hybrid" licenses of patents and trade secrets) is still possible. An underlying benefit of trade secret protection is the lack of a specific definition. However, any licensee needs to be satisfied that it is receiving a genuine trade secret and not something already in the public domain, and thus clear definition is required in the agreement. From a licensor's perspective, any license involves disclosure and the licensee might become a competitor or the licensee's employees may become a source of "leakage" of the trade secret. In any event, the licensing of a trade secret puts significant pressure on both the licensor and licensee to ensure robust confidentiality provisions are in place. An admirable, but not always an easily achievable objective.

Other factors emerge when the owner intends to commercially exploit and market the invention to external parties. In any event, the licensing of a trade secret puts significant pressure on both the licensor and licensee to ensure robust confidentiality provisions are in place.

The purpose of thi s article is not to favor one protection mechanism over the other. Rather it is intended to identify several factors and issues the owner of a technological innovation should consider. As can be seen, there are many competing possibilities across these options. Factors such as the nature of the invention, nature of the industry (size, location / geography, competitors, product lifecycles, etc.), anticipated technology lifespan, value of the invention (price point, profit margin, addressable market size etc.), supplier requirements, employee issues and the owner's business objectives are likely to shape the ultimate decision. We trust that this article provides a useful framework upon which to assess these options.

The Dennemeyer Group provides a wide range of IP protection and management services to clients throughout the world. As a result, Dennemeyer is particularly well placed to advise business owners on strategies for the overall protection of their intellectual assets, including the development and implementation of trade secret protection strategies consistent with protection through established IP registration regimes.

How to craft an effective CDA – the essentials

Dr. Dallas Wilkinson, John Walker / May 14, 2021

In our earlier article, Trade secrets – the need to be systematic, we discussed the use of Confidential Disclosure Agreements (CDAs), also known as non-disclosure agreements (NDAs). These contracts play a meaningful role in safeguarding trade secrets and other confidential information by facilitating and controlling their limited distribution. Here we will discuss the relevance of CDAs, their essential components and situations in which they are used.

CDAs are generally best used for information not in the public domain, which has been shared with specific recipients that may use it for commercial gain through subsequent arrangements. In a broad sense, these contracts have two principal purposes. First, they clearly explain that the information to which they pertain must be kept confidential. Secondly, a properly drafted CDA provides a foundation for taking legal action when trade secrets or other confidential information have been misappropriated. In order to establish a successful action before a court, proof is needed that the information covered by a CDA was:

1. Secret or not generally known
2. Important and had a valuable economic benefit to its owners (and competitors thereof)
3. Protected by the owner by taking all reasonable measures

4. Ultimately used for other parties' benefit through improper means

While "improper means" must be established through other evidence and investigation, a well-crafted CDA can go a long way in determining the other three requirements.
This article aims to provide practical insights into the issues to consider when preparing a CDA and the realistic obligations derived from receiving confidential information. We have not included any draft clauses or templates for a CDA, but recommend readers take into account the principles contained herein. We also recommend that CDAs be prepared by the relevant parties' IP attorney – most likely that of the disclosing party.

Guiding principles

In creating a CDA, there first needs to be insight and understanding into the objectives of the disclosing and receiving parties. While not mandatory, it is often best for the discloser to adopt the view of seeking obligations that they would be prepared to accept. This should facilitate more rapid execution of the CDA. With this as an underlying principle, there are essentially four elements that need to be considered when preparing the CDA:

1. The definitions
2. The essential components
3. The situation-specific components
4. The legal aspects (namely duration of obligation and jurisdictional aspects)

Definitions

The definitions comprise the specification of each party to the CDA. Key questions include:

1. Does the intended discloser (a party to the CDA) own the information being disclosed?
2. Who is / are the intended recipient(s)?
3. Is the intended recipient the correct party?

These questions might seem trivial, but in situations where the relevant parties might be subsidiaries of larger corporate organizations, such clarification is critical.

In a broad sense, these contracts have to first clearly explain that the information they pertain must be kept confidential. Secondly, they must provide a foundation for taking legal action when trade secrets or other confidential information have been misappropriated.

Another vital element of the definitions centers around the information being disclosed, as the other components will ultimately be based on this information. Typically, an agreement might set out that the discloser represents it has *"information relating to… (the Information)."* This "Information" then sets the basis of the majority of rights and obligations that follow in the CDA. The other element requiring definition is the purpose of the disclosure. This might be *"to evaluate whether or not the recipient wishes to enter into negotiations to acquire commercial rights to the Information (the Purpose)."* Once this is clearly defined, it must be spelled out that the recipient is only obtaining rights for the specific purpose(s) as defined — e.g., only an initial evaluation and without any commercial rights.

Essential elements

The essential elements focus on the disclosure and resultant obligations. A suitable analogy is that of "the black box." The discloser indicates to the recipient that it will permit looking into the black box provided the recipient is bound by non-disclosure and non-use obligations. The recipient might then comment, *"I accept that, **BUT** what if I already know what is in the black box, or if what I see is in the public domain?"* The discloser would typically respond, *"I accept that, **BUT** only if you can prove this knowledge."*

This summarized dialogue explains the basis of the key obligations in the CDA. These essential elements generally include:

1. The obligation to keep confidential and not to use [the information]
2. Reference to the "exceptions" where the recipient already knows the disclosed information, or it is in the public domain
3. A requirement of the recipient to prove it is entitled to claim such exceptions
4. The obligation of the recipient not to make any copies of the disclosed information and to return all disclosed information to the discloser (or delete if electronic) immediately upon request, and only to use the disclosed data for the defined purpose

After covering the "basics" of the disclosure, specific issues relating to it should then be considered. Such specifics will be influenced by the nature of the material being shared, the purpose of the disclosure and the recipient's characteristics. In its simplest form, a technical disclosure may be a single document labeled *"provided to recipient on [specific date]."* Where multiple written disclosures are made over a given period of time, the CDA must specify that any written disclosures during this period be labelled accordingly. A verbal disclosure may be made in some circumstances, and the CDA should reflect that such oral disclosures are confirmed in writing by the discloser within a specific time frame.

The recipient

A CDA that merely identifies the recipient may not be sufficient when the contract pertains to a technical disclosure that enables an assessment before entering into a commercial arrangement. This is particularly relevant when the recipient is a large multi-business corporation.

In this case, a prudent approach might be to limit the disclosure to only those employees with a "need to know," specifying the employees by name if necessary. The next level might be for the recipient to provide the discloser with a list of employees who have received the confidential information. In addition, a CDA may require the recipient to ensure that every employee with access to the disclosed information signs that they have read and understood the obligations of secrecy set out in the CDA.

While not an exhaustive list, these two specific variations — format of disclosure and extent of recipient's obligations — demonstrate the need for the discloser to carefully consider technical and business considerations and not simply the fundamental legal rights and obligations.

CDAs must do more than identify the recipient, especially if it is a large multi-business corporation. Two specific variations demonstrate the need for the discloser to thoroughly analyze technical and business considerations: format of disclosure and extent of recipient's obligations.

The period

Determining a suitable period of confidentiality calls for particular circumspection. The discloser must balance the need to complete a proper assessment with the demands such conditions will place on the recipient. Too short a period imparts unduly onerous requirements, while too long a duration may damage trust or hinder the very cooperation sought through the disclosure. Review of the technical and business issues is just as beneficial in the determination of period as well as the specification of recipients.

If the disclosure is related to a fast-moving technology field (e.g., software) or will ultimately be disclosed in a published patent application, a fixed period of five or 10 years might be appropriate. When the disclosure is an intended precursor to a more formal commercial arrangement, such as a license, a clause that sets a period as *"x years, or the expiration of confidentiality obligations in a subsequent commercial agreement, whichever is later"* might be more fitting.

In situations where an identifiable trade secret is at issue — for instance, the Coca-Cola formulation — the discloser may wish to make the period of confidentiality open-ended, lasting as long as the information remains a secret. Alternatively, one could separately classify some of the CDA as "confidential information" and other elements as "trade secrets," assigning a defined period of nondisclosure for the former and keeping the latter open-ended. Such a split does, however, obligate clearly and unambiguously defining these components.

Governing law

The choice of governing law and jurisdiction in a CDA, while not compulsory, is a decision that should be carefully undertaken if the discloser and recipient are not domiciled in the same country. When a disclosure ultimately benefits the discloser (e.g., as a prefatory step to a licensing agreement), the choice of law and jurisdiction should be made by the disclosing party. Of course, the recipient can make a case for alternate law and / or jurisdiction, but they usually have less influence over this selection. From a practical perspective, two factors that can influence this choice are **convenience** and **enforceability**. We will cover this area in more detail in our next article of this series, when we focus on several major jurisdictions and how they enforce trade secret misappropriation.

Completion

Once the CDA is prepared and reviewed to ensure it covers all desired aspects, every party should sign it before any information is shared, and all involved must receive a signed copy. A follow-up on the terms agreed in the CDA (and the recipient's progress in analyzing the information) is recommended, especially if the CDA's period exceeds six months. When the period expires, a separate follow-up is required to guarantee that all information shared is either returned or destroyed as agreed. Alternatively, an extension can be granted, along with any new or adjusted conditions or amendments agreed upon and signed by all parties.
As stated, this article intends to provide some insights into what preparing a CDA entails. With this in mind, it should be noted that the disclosing party ordinarily prepares a CDA, as it is their information at stake. That said, there may be circumstances under which the recipient prepares the document. Either way, the principles and practices identified above should be followed before the final CDA is executed. Accordingly, while this article is not intended as legal advice, companies either disclosing or receiving confidential information should reflect on these principles and reach out to a well-established IP services provider to obtain the most relevant advice for their unique situation.