Seven steps for securing trade secret value in IP deals

McAndrews, Held & Malloy Ltd
Wil Rao and Robert A Surrette

Yearbook 2020

Building IP value in the 21st century


McAndrews
EXCEPTIONALLY DRIVEN
to deliver smart and practical solutions to your complex IP challenges.
Focused on all aspects of the procurement, litigation and leveraging of IP rights, McAndrews has built a distinguished reputation by assembling an exceptionally talented team with an unrelenting drive to deliver. Our attorneys, patent agents and scientific advisors offer our clients an intense concentration on IP and complex technology law, as well as strong business sense and strategic ability. Experience our approach to extraordinary, personalized service and our passion for the practice of IP law.
mcandrews-ip.com

Seven steps for securing trade secret value in IP deals

By Wil Rao and **Robert A Surrette**, McAndrews, Held & Malloy Ltd

Securing optimal IP value in transactions involving the sale of either IP assets or IP-holding enterprises is serious business. Indeed, AON recently reported that intangible assets represent 84% of the S&P 500's value: $21 trillion. In the past 12 months in the United States, LexisNexis analytics has reported that $1.47 trillion in deal volume occurred across all businesses.

However, more often than not parties to IP deals do not take trade secrets seriously, leaving them largely to boilerplate non-disclosure agreement (NDA) provisions and light treatment compared with registered intellectual property (ie, patents, trademarks and copyrights). This is despite the growing vulnerability of trade secrets in the digital economy, as seen beginning around 1990 with the upward trajectory of trade secret litigation in the United States (see Figure 1 showing a steady increase in US trade secret litigation).

Moreover, trade secrets can be extraordinarily valuable (eg, Coca-Cola (soft drink recipe trade secret) and Google (search algorithm trade secret)). In fact, some of the largest trial decisions in US IP litigation involve trade secrets. For example, DuPont received a jury verdict awarding $920 million in damages for trade secret misappropriation involving Kevlar technology used in such things as body armour, fibre optic cables, automotive and industrial products (*EI du Pont de Nemours & Co v Kolon Industries Inc*, 803 F Supp 2d 469 (ED Va 2011), 637 F3d 435, 98 USPQ2d 1020 (4th Circuit 2011)). The jury verdict was later reversed on appeal and settled, with Kolon pleading guilty and being sentenced to pay $85 million in criminal fines and paying $275 million in restitution.

Given the vulnerability and value of trade secrets, it is important to handle adeptly their treatment in IP deals. While there is no substitute for tapping experienced IP counsel to navigate the nuances of a specific transaction, this chapter suggests seven steps that go a long way to securing the value of the trade secrets in your next deal.

What is IP due diligence?

IP due diligence is one element of assessing the viability and value of an overall business transaction (Geoffrey Cullinan *et al*, "The Secrets of Great Due Diligence", *Harvard Business Review*, 2004).

In due diligence an experienced IP counsel closely investigates:

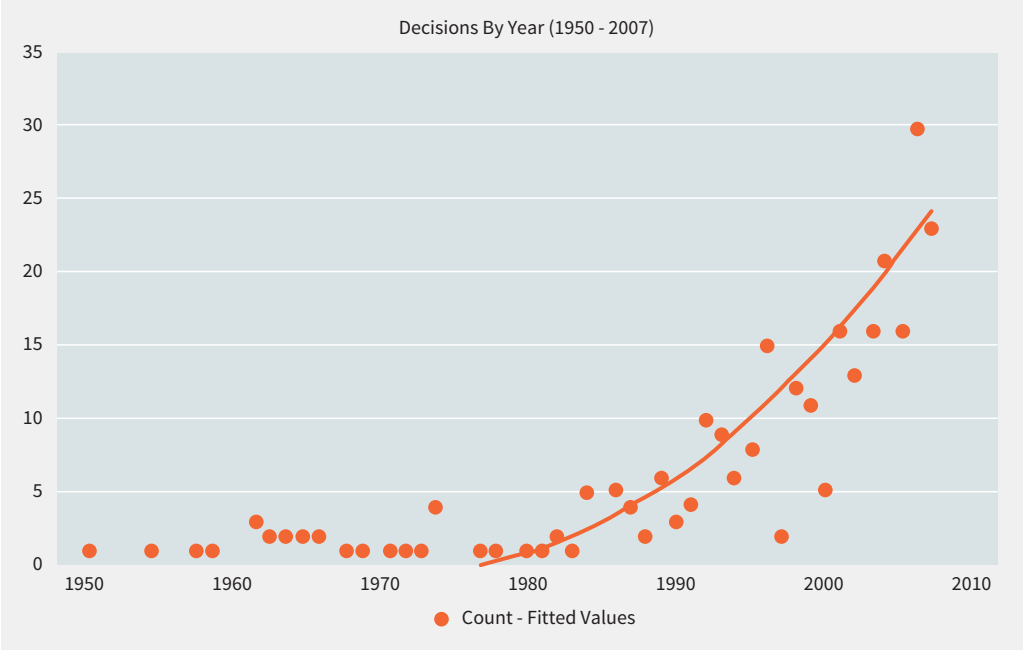
- the status of the intellectual property;
- what the IP value may be; and
- any risks associated with that intellectual property, which can include study of ownership records, encumbrances on the intellectual property and potential litigation threats.

It may also include a study of government or regulatory restrictions affecting the subject intellectual property. Of course, the depth to which IP due diligence goes depends on the nature and value of a transaction. Nonetheless, in many cases the enigmatic aspects of trade secrets makes it more difficult to use the tried-and-true methods commonly used for registered intellectual property.

What is a trade secret?

While the definition of a 'trade secret' may vary by jurisdiction, the following definition serves as a guidepost: "'Trade secret' means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value,

FIGURE 1. Almeling *et al*, "A Statistical Analysis of Trade Secret Litigation in Federal Courts", *Gonzaga Law Review*, 2010



actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." (Section 1(4) of the Uniform Trade Secret Act 1985; 18 USC Section 1836 of the Defend Trade Secrets Act 2016; and Part II, Section 8 of the Agreement on Trade-Related Aspects of IP Rights 1994.)

Trade secrets must be assessed based on the applicable jurisdiction. Virtually any type of information or knowledge may qualify as a trade secret, if it otherwise meets the definition of a trade secret. It should also be appreciated that patents are often enveloped by protectable know-how (ie, trade secrets) that contribute to the full value to the intellectual property. For example, the value of a patent on a process may only be fully realised if the know-how needed to employ the process effectively or efficiently is included in the deal.

Trade secrets may comprise technical and business trade secrets. Common examples include:

- algorithms (source or object code);
- databases;
- plans;
- secret methods;
- customer or supplier lists;
- product specifications;
- pricing;
- recipes or formulas; and
- non-public cost or pricing information.

The following are rarely considered in due diligence assessments:

- combination trade secrets, which might integrate multiple trade secrets for one purpose; and
- negative trade secrets, which might comprise a second-best way (or perhaps a failed way) of doing something.

It must be remembered that trade secrets are not always in plain sight. They can, for example, reside in the mind of an employee, perhaps in how they perform their job in a way that makes them more efficient or effective.

Seven essential steps for securing the value of trade secrets

Step 1: get with the (trade secrets) programme

Even before a deal is in the works, the seller should develop and deploy a robust trade secret

Wil Rao
Shareholder
wrao@mcandrews-ip.com

Wil Rao is a shareholder at McAndrews and a registered patent attorney. His practice focuses on litigating, procuring and developing IP rights across a wide range of technologies. He has represented clients ranging from Fortune 500 corporations to small start-ups and individuals. Mr Rao is a valued IP adviser and has provided strategic IP counselling in many areas; from patent prosecution, written opinions, re-examinations, licensing and acquisitions, to successful multi-venue, multi-patent, multi-party patent litigation at trial and appellate levels. He has represented clients across a wide range of IP rights – utility and design patents, trade secrets, trademarks, trade dress and copyright – and has worked in numerous technology areas.

Robert A Surrette
President
bsurrette@mcandrews-ip.com

Robert A Surrette, president and shareholder at McAndrews, focuses his practice on the resolution of IP and technology-related disputes, with an emphasis on patent, trademark, trade secret and trade dress litigation. For the past 15 years, Mr Surrette has managed the IP work for a leading global medical device manufacturer, handling numerous litigation and transactional matters. He has extensive experience in bringing complex IP cases to trial. He also has significant experience with multi-week trials and appellate proceedings, including arguing at the Federal Circuit. Mr Surrette maintains an active transactional practice through which he advises clients on mergers, asset deals, licensing and other matters. He also provides clients with guidance on patent portfolio development and management.

programme. The programme should include rules that define, categorise, take inventory of and secure the trade secrets. It should also actively ensure regular employee training and compliance with the programme. The level of sophistication of such a programme will depend on, for example:

- the number of trade secrets;
- whether the company has a one-way or two-way sharing of trade secrets with other companies;
- whether the company's trade secrets involve the European Union, the United States or other country markets; and
- whether the company expects a future merger, acquisition or divestiture.

It can be helpful to write trade secrets out like a patent claim and to grade their value as high, medium or low.

Security measures must be put in place to ensure that each of the defined trade secrets is appropriately protected from becoming exposed. The security level could be decided based on the trade secret value to the business and the investment available, but should clearly define:

- who has access;
- what, where and how access is and is not permitted; and
- what other physical, IT and administrative security measures are to be deployed.

In addition, companies must regularly train and educate employees regarding the rules applying to trade secrets and their importance to the business. Topics addressed should include security measures (including those related to employee hiring and exiting) and programme compliance.

Step 2: employ an NDA

An NDA is significant to getting things right from the start. Trade secrets should be a driving part of these agreements.

In general, an NDA protects the confidential information of the seller, and sometimes the buyer, from being disclosed outside of the deal. The ideal elements differ for each party to the transaction.

Some considerations for provisions on the buyer's side include:

- defining what the trade secret information and its scope is for purposes of the deal, which may be different from the seller's definition;
- deciding the extent to which the buyer will isolate its own development and trade secrets from being tainted by the seller's trade secrets that will be shared in the deal, which may require employing a separate third-party agent to review the trade secret information without the direct involvement of the buyer;
- identifying exclusions for information that is not secret;
- defining a procedure for documenting the exact confidential information exchanged orally;
- setting a term for the NDA (the seller may object to limiting the term); and
- securing a right to freely exploit information remembered following the NDA's termination – a so-called 'residuals clause', recognising that such a clause may be highly objectionable to the seller if the trade secrets are, for example, susceptible to memorisation.

On the seller side, the reality is that they must negotiate an NDA by expecting that the deal will not go through (after the buyer takes a look at the seller's secrets). Some considerations for provisions on the seller's side include:

- defining what the trade secret information and its scope is for purposes of the deal, which may be different from the buyer's definition;
- restricting access to confidential information, which may call for a clean-room approach that tightly controls access to confidential information and rigorously logs exposure (eg, name, date, time and duration);
- building multiple walls around the confidential information and secrets, which may include a phased disclosure of the trade secrets with each phase providing increasingly more and more disclosure of a higher and higher degree of sensitivity as milestones are reached;
- limiting the buyer's ability to conduct testing or analysis of the trade secrets shared during the NDA;
- prohibiting the recruitment or raiding of the seller's employees; and
- providing for dispute resolution (eg, litigation and mediation) mechanics by identifying a favourable jurisdiction and strong remedies (eg, immediate and permanent equitable relief).

Step 3: assess and test the seller's trade secret programmes, policies and governance

The buyer should review all formalised policies involving the seller's trade secrets and confidential information. Such review should test for reasonableness and ensure that compliance has historically occurred.

The buyer will want to look for a range of procedures in the policy that would reasonably eliminate or minimise detrimental leakage. For example, a strong policy might require employees exiting the company to cease all work immediately, or ask such employees to return confidential information when leaving a company. It may even require marking all trade secret documents confidential, or limiting access to, shredding or locking down such documents if conditions are met. The buyer will want to look for policies on physical access to the trade secrets and to review special IT-oriented protections such as:

- isolating computers or networks from the Internet;
- electronically dividing the trade secret information into parts;
- establishing computer dual-factor password

"An NDA is significant to getting things right from the start. Trade secrets should be a driving part of these agreements"

authentication; and
- prohibiting mobile phones from areas where trade secret information is stored.

If merited (typically where no policy exists), interview key personnel and third-party partners to assess whether an established informal policy has been followed.

Step 4: review seller's list of trade secrets to see if they meet the definition

In general, the buyer should obtain and review all documents listing and describing the trade secrets. The buyer should look to find for each trade secret at least:
- a shorthand description;
- a classification of its importance to the business;
- the 'inventor' of the trade secret;
- the creation date of the trade secret;
- who is responsible for securing the trade secret; and
- what level of importance the trade secret enjoys.

The buyer should also learn:
- what access limits the seller has placed on the trade secrets in view of the particular level of importance;
- who has had access;
- what other measures are in place to protect the particular trade secret; and
- the log of access to the trade secrets.

Step 5: review seller's agreements executed to safeguard the trade secrets

Employee agreements that address trade secrets tend to be strong evidence of both ownership and the fact that the owner has exercised reasonable measures to protect their trade secrets. These agreements must be reviewed.

An important purpose of reviewing these contracts is to determine whether the inventors of trade secrets have agreements requiring assignment of the trade secrets to the company, including work developed using company resources. Proper assignment will help confirm the seller's ownership.

Review of such agreements serves another important purpose. It ensures contractual measures were in place with all exposed employees, agents and third-party partners (including joint venturers, suppliers, distributors and even customers) that maintained secrecy.

Ideally, these agreements (and the policies reviewed above) would also demonstrate that the seller consistently restricted access to the trade secrets on a need-to-know basis. Further, these agreements should be checked to confirm that the employees, agents and third-party partners acknowledge their access to trade secrets and other confidential information.

Step 6: review physical and digital measures safeguarding the trade secrets

Restricting or controlling access to trade secret information through physical or electronic means is further evidence of the seller taking reasonable measures to protect the trade secrets. Of course, the buyer must first determine where the trade secrets are kept, identifying all physical and virtual locations (including in the mind of an employee).

Once the seller identifies a location, the seller's physical security applied to that location in view of the importance of the trade secret should be reviewed, for example:
- Are all rooms locked?
- Is key-card-controlled access limited to those who need to know?
- Is the building monitored by guards?
- Are there sign-in documents or scan-in procedures for all parties who enter spaces containing trade secrets?
- Are there fences around the building and the entire business complex?
- Are the grounds monitored with cameras?
- Are the entrances guarded by security personnel?

On the IT side, the seller's information technology and IT policies involving the trade secrets should be reviewed. The buyer should inspect what policies the seller has in place to protect its trade secrets across IT platforms, and it should also review the electronic devices where trade secrets can be accessed, in whole or in part. The goal is to determine the security applied to mobile devices, office computers and servers, along with the internet connectivity of those devices. The buyer should review any IT logs that track employee downloads, uploads and transfers that could include trade secrets and confidential information files during relevant periods.

Step 7: remaining tasks

While the first six steps will go a long way to add value to due diligence, there is more (some would say much more) that remains to be done:

- Assess the trade secret's strength (ie, whether the trade secret is easy to reverse engineer, is generally known or is otherwise rendered an invalid trade secret because it is already readily ascertainable).
- Interview the seller's employees (eg, R&D, legal, HR and IT departments) and third-party partners responsible to evaluate the seller's physical, IT and administrative protection of the trade secrets.
- Review whether there have been any key personnel arriving from or leaving the seller's competitors.
- Review paper and electronic files of key personnel involved with the trade secrets.
- Analyse records of internal and external trade secrets enforcement efforts.
- Study litigation and litigation threats against the business areas covered by the trade secrets.
- Assess the trade secret's value in view of the due diligence.
- Plan for post-closing integration and alignment with the buyer's policies and close gaps between the buyer's and seller's policies, if any, at closing.

With what the buyer and seller have at stake in these deals, handling trade secrets with heightened care is highly advisable. By following these steps and employing the level of care commensurate with the value of the trade secrets at hand, a business can protect itself before, during and after key transactions. *iam*

McAndrews, Held & Malloy Ltd
500 West Madison Street
34th floor
Chicago IL 60661
United States
Tel +1 312 775 8000
Fax +1 312 775 8100
Web www.mcandrews-ip.com