

Trade secrets in the United States

By **Dawn Rudenko Albert**, Dickstein Shapiro LLP, New York

What can be defined as a trade secret in your jurisdiction?

There is no statutory definition of a trade secret in the United States. However, there is a trend towards achieving some uniformity, with 46 states having adopted various statutes modelled after the Uniform Trade Secret Act (UTSA). The UTSA is a model law drafted by the National Conference of Commissions on Uniform State Laws. States that have not adopted the UTSA (eg, New York), have adopted their own state statutes and/or continue to apply common law.

The UTSA basically codifies the common laws relating to trade secrets and is consistent with court decisions defining what constitutes a trade secret: “Trade secret’ means information, including a formula, pattern, compilation, program device, method, technique, or process, that: (i) derives independent economic value, actual or potential, (ii) 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 (iii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.”

However, because each state defines the scope of its trade secret protection differently, courts may (and often do) reach different and even contrary conclusions concerning what constitutes a protectable trade secret. Nevertheless, US courts have found technical and non-technical information to be trade secrets, including formulae, recipes, customer lists, business know-how, business operations information (eg, pricing, product development, business

objectives, marketing strategies), internal machines or methods of production and blueprints. Courts have also denied protection to common information or procedures, including lemonade recipes, cooking procedures for barbecue chicken and customer lists posted on a company website.

What level of protection is afforded to trade secrets?

Unlike patent law, which is set by Congress and applies to all states, each state sets the scope of its trade secret protection. Some states have broad protections (eg, Massachusetts), while others have more narrow protections (eg, California). Regardless of which laws or statutes a court applies, information rising to the level of a trade secret is afforded significant protection by the courts, with such protection generally lasting for as long as the information is reasonably maintained as secret.

How willing are courts to enforce trade secret protection?

US courts are more than willing to enforce trade secret protection and routinely do so. However, courts strictly scrutinise trade secret violation claims as they are loath to restrict a person’s ability to work in a chosen industry or limit the use of information in a particular industry. Thus, courts attempt to balance the right of a company to protect its valuable confidential information with the rights of others to use readily accessible data (eg, a compilation culled from public information) or experience gained from years of employment in a specific industry.

For example, courts will not hesitate to invalidate an overreaching non-compete agreement – one of two types of contract

widely used by companies to protect their trade secrets (the second being non-disclosure agreements). A non-compete agreement restricts a former employee or partner from working for a direct competitor or otherwise competing with the company for a specified period of time. The theory behind this type of agreement is that the secret will retain its value only for a short period of time (eg, because technology advances quickly). Applying a “rule of reason”, courts will invalidate non-compete agreements if the terms are not reasonable in scope, duration and territory. For example, a non-compete agreement that seeks to prevent a former employee from working for any competitor for five years likely will be deemed unenforceable. On the other hand, a one-year restriction on working for direct competitors within a five-mile radius will likely be enforceable.

Again, the enforceability of these (and other) types of trade secret agreement will depend on the relevant jurisdiction. For example, depending on the circumstances, California either heavily restricts or completely bars non-compete agreements. Californian courts do not use a rule of reason approach, but rather require proof that the non-compete agreement is absolutely necessary to protect a company’s trade secrets. Armed with this knowledge, California companies must be more creative in seeking to protect their valuable trade secrets.

What level of proof do courts require in order to find that trade secrets have been violated?

To prevail in trade secret litigation, trade secret owners must prove five primary factors:

- Economic value derived.
- Reasonable secrecy measures taken.
- Data not readily ascertainable.
- Access by the accused.
- Notice to the accused.

Economic value can be actual or potential, and may be established through evidence showing increased revenues or profits. It also can take the form of enhanced competitive positioning (ie, reducing a competitor’s ability to compete effectively against the trade secret owner).

As to keeping a trade secret secret, there is no magic formula that courts apply in making this determination. Instead, they will generally consider all circumstances surrounding the matter; and whether the company uses reasonable measures to

safeguard its trade secrets. Absolute measures preventing access and dissemination are not required; instead, regularity and consistency in how the company protects its trade secrets are more likely to carry the day. Indeed, courts have considered many factors, including the presence or lack of fences, general access restrictions, locked doors, warning sign postings and visitor access restrictions.

The readily accessible, access and notice prongs are somewhat intertwined. Only persons who gain confidential information in confidence can be prevented from using it. Accordingly, the plaintiff must show that the accused party had access to information that is not publicly known or readily obtained, and that it had notice of the confidential nature of that information. Evidence that the accused was a former employee and that all materials relating to the information were labelled “confidential/proprietary” will likely satisfy the access/notice prongs.

What remedies are available once a court finds that trade secrets have been violated?

Several potential remedies are available to trade secret owners, including injunctions, lost profits (calculating these requires a historical baseline), unjust enrichment, reasonable royalties and punitive damages, including attorneys’ fees (wilful and malicious acts).

Criminal remedies are also available for certain types of trade secret theft. The Economic Espionage Act of 1996 makes the theft of a trade secret a federal crime if an individual or company misappropriates (or conspires to misappropriate) commercial information intending either to benefit a foreign power or to injure a trade secret owner. The penalties for such conduct include fines of up to US\$10 million for companies and US\$500,000 and up to 15 years in prison for individuals. There have been numerous convictions under the act.

When might companies opt for trade secret protection over patent protection?

To maintain a trade secret or to seek patent protection: that is the question. The answer is anything but clear-cut and requires consideration of numerous complex factors. What is the nature of the subject matter to be protected? Can it be maintained as a secret? Can it be reverse engineered? Can it be independently developed? What is the potential market value and the duration of



Dawn Rudenko Albert
Partner
Dickstein Shapiro LLP
New York
Tel +212 277 6500
albertd@dicksteinshapiro.com.

Dawn Rudenko Albert, a partner in Dickstein Shapiro LLP's IP practice, focuses on patent, trademark, trade secret and copyright litigation. Her practice involves IP due diligence in an M&A context, licensing in transactional and litigation contexts, and counselling clients in the protection, evaluation, and commercialisation of their intellectual property. Moreover, Ms Albert has extensive experience with e-discovery and is on both the Litigation/eDiscovery Steering and Quality Assurance Committees.

that value? Is that value balanced by the investment required to patent and enforce it? Depending on the answers to these (and other) questions, both types of protection have advantages and disadvantages that must be carefully considered before opting for one over the other.

For instance, the nature of the information may dictate the answer, as the scope of protectable subject matter differs between the two. While all patentable subject matter can constitute a trade secret, the opposite is not true. Trade secrets may include technical and non-technical information such as business strategies or client lists – essentially, any confidential information that derives a value to the company. Patent protection is typically restricted to novel technical innovations or improvements to inventions.

The scope of protection between the two also differs. Trade secret law does not prevent others from reverse engineering or independently developing the same invention or product technology. Patent protection, on the other hand, can be enforced against someone who independently develops or reverse engineers a patented invention. But because patents must be made public, competitors can see what a company has been developing and may attempt to develop around the patented technology.

A third significant difference is the duration of protection. Trade secrets continue for as long as the information is kept secret, whereas patent protection is generally limited to 20 years from the date that the patent is issued.

These are just three of many issues (eg, costs associated with acquiring and enforcing each, and the recent US decisions narrowing the scope of patent protection) that should be considered before choosing one type of protection over the other. The bottom line is that there is no decisive advantage in choosing one form of protection over the other. Numerous legal and business decisions will affect the choice to keep information secret or to seek a patent. The key is to analyse each element carefully and choose the protection that best suits the subject matter and the goals and limitations of the business.

Can trade secret and patent protection be used in conjunction?

Trade secret and patent protection cannot be used in conjunction relating to the same invention or data because the patent process requires public disclosure of the

invention, whereas trade secret protection requires that the information be kept secret. Accordingly, once a patent application is published (which is generally 18 months after filing), the secret is public and no longer protectable. This is true even if the patent is ultimately denied. There is no legal mechanism to put the cat back in the bag; once it's out, it's out, and there are no means to prevent other innocent persons from using the now public information.

This should serve as another reminder that the decision to maintain something as a trade secret or seek patent protection should not be taken lightly.

How are trade secrets best protected in a licensing context?

Once again, there are advantages and disadvantages to licensing. An obvious advantage is the potential to increase revenue. Several less obvious advantages are the potential for cross-licensing and acquisition of new technologies without corresponding research and development expenses.

There are also a number of potential disadvantages to licensing trade secrets – the most obvious being the loss of a trade secret. Trade secrets must be zealously guarded. If a licensee fails to do so, the trade secret is lost – even if by no fault of the licensor–trade secret owner. Accordingly, if the decision to license a trade secret is made, it is imperative that the agreement be carefully crafted to ensure that the strongest possible protection is afforded to those licensed secrets.

A common and disastrous error made by companies is to use a generic licence agreement or identify generic categories of material to an agreement. To protect fully confidential information, each individual secret or group of secrets must be expressly set out in the agreement. Courts strictly scrutinise trade secret claims and a claim that everything is confidential often results in a ruling that nothing is confidential.

All obligations, restrictions and conditions should be expressly set out in the licence. The terms should include provisions relating to ownership, assignability, scope of use and security measures to protect the confidential information. It is essential that the agreement also conform to the trade secret laws of the licensing state (or foreign jurisdictions, which have their own legal nuances and requirements).

The moral of the story here is to be precise. The more specific the licence

regarding obligations, restrictions and the identification of the trade secrets to be licensed, the stronger the protection and enforcement that such agreements will receive.

What are the key issues to bear in mind when developing a trade secret policy?

The key to developing a strong trade secret policy is to perform a soup-to-nuts analysis. This is truly a situation where the devil is in the detail. Far too often, companies expose themselves to damages claims or lose a valuable secret because they fail to develop a proper trade secret policy.

The most critical element in protecting trade secrets is keeping them secret. This sounds simple enough, but maintaining information as secret is not as straightforward as one might think. For instance, courts have found no trade secret protection where third parties had access to a company's rubbish bins.

Companies tend to overlook many issues and areas that, if addressed, would more fully protect their trade secrets and themselves from potential liability. The following is a brief list of the provisions that should, at a minimum, be included in any trade secret policy:

- New and exiting employee policies. These include employee agreements, entrance and exit interview protocols and agreements (eg, new hires from competitors – does the company minimise its risk of suit when hiring laterals from a competitor relating to trade secrets?); employee-exit reminders regarding trade secrets; procedures to maintain and cull former employee data; non-compete provisions; and training to educate employees regarding what can and cannot be distributed and discussed outside the company, and to help employees to identify new trade secrets and use proper security procedures.
- Screening policies. All materials to be transmitted or disclosed to the public or third parties – including marketing/advertising materials, sales pitches, demonstrations, publications and speeches – should be screened for confidential information.
- Security policies. These include access and control of trade secret information (eg, through passwords, data disposal or locked areas); notice of proprietary information (eg, by labelling and marking all confidential materials, products and documents), posting signs and other reminders; and a periodic

review of security policies and procedures to ensure compliance throughout the company.

- Licensing (in and out) policies. Companies should inventory and periodically review confidential user licences, intranet user screen notifications, disclaimers and the like. In addition they should confirm that all obligations to maintain third-party licensed trade secrets are being met and that licensees are fulfilling their obligations to maintain information as secret.
- Monitoring policies. Companies should conduct periodic external portfolio monitoring of valuable trade secret materials and also monitor competitors for unauthorised use or misappropriation of company trade secrets.

Are there any other issues that you would like to raise?

The potential benefits and risk exposure relating to trade secrets cannot be overestimated.

Because of the significant number of nuances in US law relating to employment restrictions, ownership rights, implied duties to maintain company information confidential, scope of protection and enforcement of trade secrets, it is highly recommended that counsel be consulted before finalising any agreement or developing any trade secret policies. Choosing the wrong protection or failing to properly protect a trade secret may have dire consequences and is often irreversible. ■

Dickstein Shapiro LLP
1633 Broadway
New York, NY
10019-6708, United States
Tel +1 212 277 6500
Fax +1 212 277 6501
www.dicksteinshapiro.com