Trade Secrets

A Guidebook for Technical and Business Professionals

by Claire Laporte and Emma Winer

FOLEY HOAG LLP

Contents

Trade Secrets

A Guidebook for Technical and Business Professionals

by Claire Laporte and Emma Winer

Introduction

Trade secrets can be a valuable component of an intellectual property (IP) portfolio, whether as a complement to patents or as an alternative. Trade secrets are fundamentally different from patents and must be protected in fundamentally different ways. Trade secret protection is available for a broad array of information for which patents are not available. Conversely, some innovations cannot be protected as trade secrets but can be patented.

Although trade secret protection can provide an economical and effective means to protect a company's information, it is critical to act prospectively to preserve trade secrets. Taking precautions with employees, vendors, and business partners now can avoid costly losses in the future.

In 2016, Congress passed a new federal law governing trade secrets: the Defend Trade Secrets Act of 2016 (DTSA). This statute creates a new federal civil cause of action for misappropriation of trade secrets. It supplements, rather than

preempts, state trade secret laws, which vary from one jurisdiction to another.

This publication is intended to provide general guidance on the law of trade secrets. It is not a substitute for the analysis that must be undertaken to assess any particular situation.

Chapter 1

What Is a Trade Secret?

In the past, trade secrets were protected principally under state law. All but two states have adopted a version of the Uniform Trade Secrets Act (UTSA). However, because those versions differ slightly from state to state, "Uniform" is a misnomer.

In 2016, Congress passed the DTSA, which empowered companies to sue parties that misappropriate their proprietary information. The DTSA, which amends the Economic Espionage Act (EEA), defines trade secrets in a way that is broadly consistent with the UTSA. The passage of the DTSA supplements state-law protections for trade secrets.

The EEA, as amended by the DTSA, defines trade secrets as:

> all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
>
> > (A) the owner thereof has taken reasonable measures to keep such information secret; and
> >
> > (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper

> means by, another person who can obtain economic value from the disclosure or use of the information ….

Whether under the DTSA or under state law, the key factors are that a trade secret is:

- Not generally known to the public (or in the relevant industry);
- Economically valuable because it is not known; and
- The subject of reasonable efforts to maintain its secrecy.

Some jurisdictions also require that the trade secret be in continuous use.

Examples of Information that can qualify for trade secret protection:

- Scientific data
- Manufacturing drawings and methods
- New product concepts or design
- Pre-clinical or clinical data
- Ingredient formulas and recipes
- Business information (e.g., business plans, budgets, forecasts)
- Software source code and overall design
- Customer lists or compilations of information
- Supplier lists

Examples of information that does not qualify for trade secret protection:

- General industry skills and knowledge
- Abstract ideas or goals

- Publicly available information

Just because a company considers information a secret does not guarantee that a court will recognize that information as a trade secret under the law. Trade secret lawsuits often focus on whether the information is in fact a trade secret and, if so, whether it was wrongfully taken. Several steps discussed in this publication can increase the likelihood that information will qualify as a trade secret.

Chapter 2
Trade Secrets Versus Patents

Trade secrets and patents are both intellectual property, but they differ in key ways that are summarized in the table below.

Trade Secrets Versus Patents at a Glance

PATENTS	TRADE SECRETS
Require public disclosure	Destroyed by public disclosure
Term: 20 years	Term: as long as you keep the secret
Can protect reverse-engineerable items	No protection against reverse engineering
Obtained by prosecution; maintained by payments	Can be labor-intensive to maintain; requires reasonable efforts to keep secret
Exclusive: no unlicensed use permitted	Non-exclusive: use prohibited only if it results from misappropriation
Must be non-obvious, adequately described, and useful	Must acquire value from not being generally known

Trade Secrets Must Be Secret

To benefit from court protection, trade secrets must be kept secret. Any disclosure of the details of a trade secret may destroy the protectability of the secret.

Patents, in contrast, are public. Indeed, public disclosure is the price the inventor pays in exchange for the government-granted temporary monopoly on the invention. In the U.S., patent applications are typically published eighteen months after they are filed, and patents are published after they are granted. An application must describe the invention and must provide sufficient detail to enable others to practice it. An inventor must also disclose the best mode for practicing the invention.

Many companies maintain their inventions as trade secrets until their patent applications or patents are published. Once the publication occurs, the trade secret ceases to exist.

Trade Secrets Are of Potentially Indefinite Duration

A trade secret need never expire. The trade secret owner can benefit from trade secret protection for so long as the information remains secret.

In contrast, patents expire after a set number of years (typically, twenty years after filing). Once a patent expires, anyone can practice the patented invention.

Trade Secrets Can Be Reverse Engineered

The law permits reverse engineering of a trade secret. In other words, a competitor can obtain a company's product on the open

market, take it apart, determine how it works, and use that information to compete.

It is not legal to reverse-engineer a patented product. Therefore, an invention that is easy to reverse-engineer is better protected with a patent than as a trade secret.

One caveat: some products are provided on a contract basis. Companies have had some success in incorporating clauses in their contracts for these products that prohibit reverse engineering or, in some cases, even prohibit disassembling the product.

Trade Secret Protection Exists Immediately Whereas Patents Are Issued After An Administrative Process Through A Government Agency

A trade secret can exist without any application being filed with any government body, and it may exist and have value from the moment it is created. To get a patent, on the other hand, an inventor must apply to the United States Patent and Trademark Office or a foreign equivalent. The patent application process can take several years.

Trade Secrets Are Non-exclusive

Many different owners can use the same trade secret so long as each one arrives at the secret through legitimate means, such as independent development. In contrast, the holder of a patent has the exclusive right to practice the patented invention.

For example, assume Company A develops a method of manufacturing computer chips that gives it a competitive advantage. Several years later, Company B independently develops the same method. If Company A has a patent, it can prevent

Company B from using its method. If Company A kept its method as a trade secret, it cannot prevent Company B from using the method so long as Company B developed the method legitimately and independently.

One risk of relying on trade secret protection is that another company can independently develop the same invention and patent it. That company could then try to enforce its patent monopoly.

Trade Secrets Can Cover Information That Is Not Patentable

Trade secrets can cover information that is not patentable. Only inventions can be patented, but many kinds of ideas and information can be kept as a trade secret. For example, sensitive company business information that has competitive value may be a trade secret even though it is not an invention. Business plans, manufacturing techniques, customer lists, and financial information may all be kept as a trade secret. Information about things that do not work in a technical field can also be a trade secret. Of course, inventions can also be kept as trade secrets – but only for so long as they remain secret.

How Do You Prove That Your Information Is A Trade Secret, and How Does That Proof Differ From a Patent Infringement Case?

TIn a lawsuit, the party claiming the existence of a trade secret has to prove that the information it thinks has been misappropriated is, in fact, a trade secret. To do that, the owner must show that it has taken reasonable measures to maintain the secrecy of the secret and must demonstrate that the secret has value by virtue of not being generally known. There are often disputes in trade secret

lawsuits about how the trade secret should be defined and what its scope is.

In addition to proving that it owns the trade secret, the owner must also prove that the other party misappropriated the trade secret. Usually, that involves proving that the other party either disclosed the trade secret or used it for its own benefit.

The issues in trade secret litigation are similar to those in a patent infringement case. Although it is easy for a patent-holder to prove that it owns its patent, there almost always are serious disputes about the scope and validity of a patent. A patent infringement plaintiff must also show that the other party is making, using, selling, or importing the patented technology.

Chapter 3

Keeping Trade Secret Information Secret

For information to be protected as a trade secret, the information must be the subject of reasonable efforts to maintain its secrecy. Reasonableness is determined on a case-by-case basis. As businesses grow, security must keep pace in order for a court to consider the security measures reasonable.

The question whether a party has made reasonable efforts usually turns on complex factual considerations including the party's use of nondisclosure agreements; controls over information flow, such as "need-to-know" restrictions on internal dissemination of information; and the nature and extent of security precautions, including electronic security, to protect the information. Any voluntary, unprotected disclosure to a third party without an appropriate nondisclosure agreement may destroy a trade secret.

Many technology companies publish information about their work, whether for marketing purposes or in published patent applications or scientific journals. Companies also disclose information at scientific meetings. Publication or public presentation completely destroys a trade secret as of the date of the disclosure. Thus, it can be important to establish that a particular piece of information was maintained as a trade secret until the moment of disclosure. It is also important to keep records of when disclosures were made.

Thus, a critical part of security is advanced planning. It is much easier to defend your trade secrets effectively and efficiently if you

develop a security strategy ahead of time. An important part of such a strategy is thinking through what information is a trade secret. Owners who think in advance about what information they want to protect stand a much better chance of getting court protection – and of preventing information loss in the first place – than companies that wait for problems to arise.

Examples of Reasonable Precautions

- Written nondisclosure agreements with employees, contractors, consultants, or contract parties specifying how confidential, proprietary, and trade secret information should be handled and used;
- Depending on the state – because there are some states that frown upon this – written non-competition agreements;
- Setting up need-to-know information access systems;
- Preventing unauthorized access to information (e.g., keeping paper documents in locked rooms or cabinets; restricting access to locations where information is stored; putting password restrictions on computer files; keeping electronic access logs to show what users have accessed information; automated monitoring to flag possible unauthorized entry into computer systems or unusual activity by authorized users);
- Sign in/sign out procedures and nondisclosure agreements for visits to your facilities;
- Educating employees about the company's trade secret policies;
- Marking physical and electronic documents that contain trade secret information as confidential;

- Implementing a computer security policy (e.g., multifactor authentication for remote access; prohibitions against downloading information to flash drives; prohibitions against working on confidential information from home except through a virtual private network); and
- Training for sales force and other employees who communicate with third parties to ensure that they do not disclose trade secrets.

Taking these steps not only helps protect trade secrets, it also makes it easier to seek protection from a court if it appears that someone is attempting to use confidential information without authorization.

Case Studies

Two cases illustrate the importance of taking reasonable precautions to keep a company's information secret. In both cases, vendor companies disclosed information about their products in the hopes of generating business. In the first case, the vendor lost control of its information because it had not taken reasonable precautions to protect it. In the second case, the vendor kept control of its information because it took reasonable precautions from the outset. Both companies had invested money in developing their information, but only the company that took reasonable precautions was able to protect its investment

In *Incase Inc. v. Timex Corp.*, 488 F.3d 46 (1st Cir. 2007), the plaintiff, Incase, was in the business of designing packaging for different products. As part of its business model, Incase designed a client company's packaging for free and relied on future orders to recoup the cost of design. Unfortunately from a trade secret

standpoint, Incase provided the packaging designs to potential customers with no strings attached. In this particular case, Timex ordered some packages for its watches from Incase, but fewer packages than Incase expected. When Incase learned that Timex had subsequently hired a Philippine company to create the Incase-designed packaging at a lower cost, Incase sued Timex. After a lengthy lawsuit, the appeals court ruled that because Incase had taken no precautions to protect the secrecy of its design, the design was not a trade secret. Timex was not liable for trade secret misappropriation for using Incase's packaging design with the other vendor.

Contrast *Incase* with the second case, *TouchPoint Solutions, Inc. v. Eastman Kodak Co.*, 345 F. Supp. 2d 23, 29 (D. Mass. 2004). There, TouchPoint entered into negotiations with Kodak to sell software for use in digital picture kiosks. Before TouchPoint disclosed information about the technology to its customer, TouchPoint and Kodak signed a Confidential Disclosure Agreement (CDA). According to the CDA, if TouchPoint labeled information as confidential, Kodak was to treat it as such. TouchPoint also obtained Kodak's explicit agreement that all information concerning the software would be confidential.

When Kodak tried to use some of TouchPoint's information in developing its own software, TouchPoint was able to win a preliminary injunction preventing Kodak from using the information. Even though the information that Kodak tried to use did not fit precisely within the information defined in the CDA, the court granted the preliminary injunction because TouchPoint had taken reasonable precautions to protect the information. This included

entering into a CDA; obtaining Kodak's explicit agreement that all information concerning the software would be confidential; password protecting the software server; assigning a gatekeeper to monitor the flow of confidential information; and having TouchPoint representatives reiterate that their disclosures were made in confidence. After TouchPoint won the preliminary injunction, the parties reached a settlement agreement. By thinking ahead about trade secret protection, TouchPoint was able to enforce its rights effectively.

Employee Agreements to Protect Trade Secrets

Three types of agreements with employees can be particularly useful to protect trade secrets and deserve special attention: nondisclosure agreements, invention assignment agreements, and non-competition agreements. These agreements are useful for protecting an owner's trade secret information and provide a legal remedy if such information is improperly disclosed.

Most companies should require their employees to sign nondisclosure agreements to ensure that employees will not share the employer's trade secrets with others during or after employment. An effective nondisclosure agreement should cover the full term of the employee's employment. It should define the confidential information, the exclusions to what is confidential, and the obligation of the employee to hold the information in confidence. Information disclosed without such an agreement is more difficult to protect as a trade secret.

To enhance the effectiveness of a nondisclosure agreement, it is helpful to discuss it during employee orientation, including when employees are promoted to new positions. When an employee leaves, the employer should hold an exit interview and remind the

employee of any obligations under the agreement. Such an interview can also lay the foundation to later prove a violation of the nondisclosure agreement. It may also be prudent to check logs of computer activity for departing employees, to confirm that the employee has not engaged in unauthorized downloading of confidential material.

Most companies should also require employees to sign invention assignment agreements. These agreements transfer ownership of employee inventions to the employer. In the event that an employee uses confidential information of an employer after leaving the employer, such an agreement provides an additional mechanism for asserting ownership and control over inventions made by the employee during employment but then taken by the departing employee to a new employer or business. Notably, some jurisdictions place some restrictions on the scope of these agreements, and so it is helpful to consult counsel to determine an acceptable scope to put in your agreement templates.

In some jurisdictions, it is also helpful to have a non-competition agreement with employees. These agreements prevent the employee from working in the same field as the employer, or in the same geographic area, for a period of time after the employee leaves. These agreements are enforceable in certain states and are not in others. The states that do not enforce these agreements consider them to be an unreasonable restriction on employee mobility. Even in states that enforce non-competition agreements, the agreement must be reasonable in scope, time, and geography. In other words, it must not prohibit an employee from seeking other employment in too wide a field of business, for too long a period of time, or for too wide a geographical area. The key is making sure

that the agreement protects the trade secret owner's information and is not merely a hardship for the employee.

The DTSA contains provisions protecting employee mobility, while respecting the diverse state approaches to non-competition agreements. It restricts the availability of court orders to "prevent a person from entering into an employment relationship," and provides that if an order places conditions on a person's employment, the restrictions "shall be based on evidence of threatened misappropriation and not merely on the information the person knows." The DTSA also prohibits issuing an injunction that "conflict[s] with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business."

The DTSA also requires that any employer-employee agreement relating to trade secrets or confidential information contain a notice of protections available to whistleblowers under the DTSA. Those protections, more specifically, are immunity from criminal or civil liability under both federal and state trade secret law for disclosing a trade secret in confidence to a government official or an attorney "solely for the purpose of reporting or investigating a suspected violation of law." Companies that fail to provide the required notice in their agreements can still sue an employee who misappropriates a trade secret, but certain enhanced remedies will not be available. Hiring "consultants" instead of employees does not remove the notice requirement. The DTSA defines "employee" to include a "contractor" or "consultant."

Chapter 4

What Is Trade Secret Misappropriation?

Misappropriation and Theft

Both the federal DTSA and the UTSA as adopted by various states define ***misappropriation*** broadly to include the improper *acquisition* of a trade secret as well as the *disclosure* or use of someone else's trade secret. Ways of improperly acquiring a trade secret can include theft, bribery, misrepresentation, breach of a contractual duty (such as a duty imposed by a nondisclosure agreement), inducement of another to breach a duty, and espionage through electronic or other means. A person who knows or ought to know that a trade secret was improperly acquired by someone else also misappropriates that trade secret if he or she then acquires it from the person who acquired it improperly.

Reverse engineering (unless done in violation of a contract) and independent derivation are not improper.

The EEA also defines outright theft of a trade secret – a federal crime – as stealing, taking without authorization, or obtaining by fraud or deception; copying, photographing, downloading, uploading, or transmitting without authorization; and receiving, buying, or possessing if you know that the information was stolen.

What Is Not Misappropriation

The law allows acquisition of a trade secret by proper means. In addition to reverse engineering and independent development,

proper means include:

- A license from the trade secret owner;
- Learning the trade secret from published literature or presentations at scientific conferences;
- Observation of the item in public use or on public display; or
- Freedom of Information Act requests for information provided in a non-secure manner by competitors.

Chapter 5
Bringing a Trade Secrets Case; Remedies

A company whose trade secrets have been misappropriated can sue the perpetrator in federal or state court. Regardless of the court, the company can seek the protection of both federal and state trade secret law, because the DTSA does not preempt state law.

There is one unique remedy available under the DTSA: it allows for an ex parte seizure process "in extraordinary circumstances" to "prevent the propagation or dissemination of the trade secret."

Two kinds of relief are available for actual or threatened trade secret misappropriation under both federal and state law. A court may grant an *injunction* (a court order) to protect the trade secret owner. A court can also grant *money damages* – payments from

the misappropriator to the owner to either repair the damage done to the owner or force the misappropriator to return wrongful gains.

Injunctions

A court may issue orders (injunctions) to a party accused of misappropriating a trade secret. For example, a court may order return of confidential documents or electronic information. A court may issue an injunction to prevent the misappropriator from:

- Continuing to use the trade secret;
- Getting an unfair head start even when the information is no longer secret; and/or
- Selling or otherwise disclosing the trade secret to others.

As discussed above, a court in some jurisdictions may issue orders relating to employment, such as preventing someone knowledgeable about a company's trade secrets from working for a competitor, or requiring a former employee to assign a patent to the former employer.

A key issue with injunctions is time frame. Courts may enter a permanent injunction prohibiting use of a party's trade secret. In situations where the secret later becomes public, however, a court might consider it unfair to prevent someone from using that public information forever. Many injunctions are for a length of time appropriate to remove any unfair advantage gained from the misappropriation. For example, someone accused of misappropriation might argue the injunction should last no longer than the time it would have taken to develop the trade secret independently.

Examples:

- Company B misappropriates Company A's secret assembly-line configuration. A court could order Company B not to use that configuration, either permanently or for some period of time.
- Company A is developing a new medical device that is not yet on the market. During discussions of a possible acquisition of Company A by Company B, Company B learns about the product design. Instead of acquiring Company A, Company B develops a similar device. A court could require Company B to delay its launch so that it does not benefit from the "head start" it gained by seeing the design when it was a secret.
- Salesperson X, an employee of Company A, misappropriates Company A's customer list by taking a copy with him when he quits. A court could order Salesperson X to return the list (and any copies), order Salesperson X not to use the list at his new company, and/or prohibit Salesperson X from working in the same geographic territory as that covered by the list.

Money Damages

Instead of or in addition to an injunction, a court may award money damages. Damages can be measured in different ways, including by:

- The trade secret owner's lost profits
- The profit the misappropriator gained
- Other unjust enrichment to the misappropriator, such as the money saved by misappropriating the trade secret information rather than developing it independently
- A reasonable royalty for the trade secret

Under the federal DTSA as well as under the UTSA, which is applicable in most states, a court may multiply the original damages award in cases of willful and malicious misappropriation. It may also be possible for the trade secret holder to recover its attorneys' fees.

Chapter 6

The Flip Side: How to Stay Clear of Other Parties' Trade Secrets

Savvy companies are aware that they could be on either side of an accusation of trade secret misappropriation. Therefore, in addition to protecting their own trade secrets, companies should implement policies to minimize their potential liability to other trade secret owners. Potential policy elements can include:

- Screening incoming employees for confidentiality, invention assignment, and non-compete obligations
- Responding (internally and externally) to cautionary letters from the former employer of a new employee
- Researching state law concerning enforceability of non-compete agreements before hiring
- Keeping documentation of the company's scientific knowledge and independent development
- Limiting the amount of third-party information that the company agrees to keep confidential
- Requiring authorization to sign third-party nondisclosure agreements
- Limiting disclosures from third parties

As with protecting trade secrets, it is better to prevent a problem than to react to a problem once it has arisen. Companies should think ahead about how they acquire information, who owns the information, and what duties they have to the information's owners.

Conclusion

Trade secrets can form a valuable part of a company's IP portfolio. This publication has identified several areas that companies should consider in formulating their trade secret policies. With proper foresight, companies can use trade secret protection to preserve their competitive advantage by keeping information confidential.

About Foley Hoag LLP

Foley Hoag provides innovative, strategic legal services to public, private and government clients across the globe. We have premier capabilities in the life sciences, healthcare, technology, energy, professional services and private funds fields, and in cross-border disputes. The diverse backgrounds, perspectives and experiences of our lawyers and staff contribute to the exceptional senior level service we deliver to clients ranging from startups to multinational companies to sovereign states. For more information, visit www.foleyhoag.com or follow @FoleyHoag on Twitter.

Claire Laporte

Claire Laporte is a trial lawyer at Foley Hoag LLP who handles patent and trade secret cases and other technology-related matters.

Claire has won numerous cases in the federal courts and in the International Trade Commission, including one in which she obtained a verdict of willful infringement against a major medical products company and another in which she convinced the International Trade Commission to find two biotechnology patents invalid. Recently, she argued before the Patent Trial and Appeal Board in five related cases concerning immune checkpoint technology.

Claire provides strategic patent portfolio counseling services and opinions on patent-related matters. She provides IP advice to companies preparing to be acquired or seek financing. Claire has lectured widely on issues relating to patents and trade secrets, including at Cold Spring Harbor Laboratories, Harvard Law School's Petrie-Flom Center, MIT, Boston University, Northeastern University, the Boston Bar Association, the American Law Institute, and other bar associations.

Emma Winer

Emma Winer is an associate in Foley Hoag's Intellectual Property department. Her practice focuses on IP litigation matters involving patents, trade secrets, trademarks, copyrights, and false advertising. While attending law school, Emma interned in the Cyberlaw Clinic at the Berkman Center for Internet and Society, where she advised clients on copyright and privacy issues. Before law school, Emma worked as a paralegal specialist in the Economic Crimes Unit of the U.S. Attorney's Office for the District of Massachusetts.

TRADE SECRETS

FOLEY HOAG LLP

BOSTON | NEW YORK | PARIS | WASHINGTON | FOLEYHOAG.COM