

# Trade Secrets

A Guidebook for Technical and Business Professionals Involved in Legally Protecting Products, Technologies and Services

by Vickie L. Henry and Claire Laporte



# Contents

<b>Introduction</b> .....	3
Chapter 1	
<b>What Is a Trade Secret?</b> .....	4
Chapter 2	
<b>Trade Secrets Versus Patents?</b> .....	6
<i>Trade Secrets Versus Patents at a Glance</i> .....	10
Chapter 3	
<b>Keeping Trade Secret Information Secret</b> .....	11
Chapter 4	
<b>What is Trade Secret Misappropriation?</b> .....	17
Chapter 5	
<b>Remedies for Trade Secret Misappropriation</b> .....	19
Chapter 6	
<b>Criminal Enforcement of Trade Secrets</b> .....	22
Chapter 7	
<b>The Flip Side of Trade Secrets: How Not to Misappropriate</b> .....	26
<b>Conclusion</b> .....	27

---

<i>About Foley Hoag LLP</i> .....	28
<i>Vickie L. Henry</i> .....	28
<i>Claire Laporte</i> .....	29

# Trade Secrets

A Guidebook for Technical and Business Professionals Involved in Legally Protecting Products, Technologies and Services

by [Vickie L. Henry](#) and [Claire Laporte](#)

## Introduction

Trade secrets can be a valuable component of an intellectual property (IP) portfolio, whether as a complement to patents or as an alternative. Companies benefit from an IP portfolio that matches the unique benefits of trade secrets and patents to the types of information they seek to protect. Trade secret protection can be available immediately, without going through a government agent, whereas a patent is available only after an application to and approval by the government. And unlike patents, trade secrets provide IP protection of potentially infinite duration. Trade secret protection is also available for a broad array of information for which patents are not available.

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

The law of trade secrets varies from state to state. This publication is intended to provide guidance to the law of trade secrets generally, and is not a substitute for individualized state and federal law analysis. As always, every situation has to be evaluated on its own merits.

## Chapter 1

# What Is a Trade Secret?

The precise definition of “trade secret” varies by state, just as other laws vary from state to state. Forty six states, the District of Columbia, and the U.S. Virgin Islands have adopted some variation of the [Uniform Trade Secrets Act](#) (UTSA) – a model law designed to simplify the principles that judges have articulated over several centuries. The UTSA defines trade secret as:

information, including a formula, pattern, compilation, program device, method, technique, or process, that:

- 1) derives independent economic value, 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
- 2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Massachusetts, New Jersey, New York, and Texas follow the older Restatement (First) of Torts Section 757, although movements to adopt the UTSA occur frequently in those states. Regardless of jurisdiction, the key factors are that a trade secret is information that 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
- Ingredient formulas and recipes
- Business information (e.g., business plans; cost/pricing data; budgets and forecasts)
- Software source code and overall design
- Customer lists or compilations of information
- Membership or employee lists
- 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. In short, trade secrets can cover information that can and cannot be patented and are *unpublished, of potentially indefinite duration, and nonexclusive*. Patents are limited to statutorily defined subject matter and are *published, of definite duration, and exclusive*.

### Trade Secrets Can Cover Information That Is Not Patentable

Trade secrets encompass a broader category than patents. Patents require *novelty*. In other words, something may be patented only if it is inventive. Trade secrets may cover an invention but may also cover information you do not want your competitors to know. Because trade secrets need not be novel, owners can sometimes benefit from trade secret protection even where patent protection is not available.

Customer lists, for example, would not be patentable but may be afforded trade secret protection. Generally, for trade secret protection a customer list must be sufficiently difficult to create. If, for example, creating the customer list requires intensive solicitation or investigation – the list can qualify for trade secret protection (assuming, of course, that the owner takes steps to keep the list secret).

### Trade Secrets Must Be Secret

To benefit from court protection, trade secrets must be protected and kept secret. Patents, in contrast, are public. Indeed, this public

disclosure is part of the bargain the inventor makes for the government-granted temporary monopoly on the invention. In the U.S., generally even applications for patents are published eighteen months after they are filed. And the patent may not be valid if the disclosure is not sufficient (the written description must be adequate, the invention must be enabled, and the application must disclose the best mode for practicing the invention).

### **Trade Secrets Are of Potentially Indefinite Duration**

A trade secret need never expire. The trade secret owner can benefit from trade secret protection so long as the information remains secret and the company owner uses it. In contrast, patents by their nature expire after a set number of years (typically, twenty years after filing). Once the patent expires, anyone can practice the patented invention.

### **Trade Secrets Can Be 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 trade secret and patent it. That company could then try to enforce its patent monopoly unless the patent is a business method patent.

### **Trade Secrets Can Be Reverse Engineered**

The law permits reverse engineering. In other words, a competitor can fairly obtain a company's product, take it apart, determine how it works, and use that information to compete. Various reasons have been articulated for why reverse engineering should be permitted. One is that the sale of the product is akin to a publication. A second is that reverse engineering spurs innovation - it encourages inventors to apply for patents and to search for patentable ideas. Therefore, if the invention is easy to reverse engineer, a patent provides superior protection to a trade secret. For those products that are not mass-marketed but are provided on a contract basis, companies have had some success in incorporating anti-reverse engineering clauses. Of course, a company that obtains a competitor's product through deception leaves itself open to a challenge of trade secret misappropriation or, at the least, may create evidence of the value of the product should the two companies subsequently be opponents in patent infringement litigation.

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

Trade secret protection is immediate whereas patent protection requires an inventor to apply for a patent to the United States Patent and Trademark Office (or a foreign equivalent). The patent

application process can take several years. Of course, trade secret protection is available unless and until the patent application publishes or a patent issues.

### **It Is Easier To Prove The Existence And Validity Of A Patent In Court**

It is easier to prove in court the validity of a patent than the existence of a trade secret. A party to litigation proves the existence of the patent by showing a “ribbon copy” of the patent as issued by the United States Patent and Trademark Office. In addition to having, literally, the stamp of approval of the Patent Office, a patent holder asserting rights in court enjoys a presumption that the patent is valid. The party challenging the patent has the burden of proving, by clear and convincing evidence, that the patent is not valid and should not have been issued. In trade secret litigation, the party claiming the existence of a trade secret has to prove the information indeed is a trade secret.

## Trade Secrets Versus Patents At A Glance

	Trade Secrets	Patents
<b>Subject matter?</b>	Information you do not want your competitors to know	Qualifying inventions that are new, useful, and non-obvious
<b>Disclosure?</b>	Must be kept secret	Require disclosure and publication  Insufficient disclosure may result in patent invalidity
<b>When are rights enforceable?</b>	Immediately	Only after patent issues
<b>Duration of rights?</b>	Potentially infinite	Fixed term, usually 20 years from filing application
<b>Exclusivity of rights?</b>	None – can be independently developed or reverse engineered	Legal monopoly
<b>Geographical scope?</b>	Potentially international	Limited to country(ies) that issued patent(s)
<b>When is one clearly better than the other?</b>	When the subject matter is not patentable (e.g., customer lists)  If the longest protection possible is best  The cost of obtaining a patent is prohibitive	When a product can be reverse engineered or is likely to be independently developed  When maintaining secrecy would not be practical  When it is important for competitors, investors or others to know about the IP and the fact you have it
<b>How can someone avoid your intellectual property rights or deprive you of them?</b>	Independently develop  Reverse engineer  Prove the information is not a trade secret  Hire your knowledgeable employees (without confidentiality obligations)  Publish the information	In the U.S., invent first and file (in other countries, file first)  Invent and publish  Design around the patent  Prove your patent is not valid (is not new; is obvious; is indefinite; is not enabled; fails to disclose best mode; has insufficient written description)  Prove your patent is not enforceable for inequitable conduct before the Patent Office
<b>How can you defeat your own intellectual property rights?</b>	Disclose the trade secret without confidentiality  Lose knowledgeable employees without confidentiality or non-compete obligations  Lax security  Apply for a patent, allow the application to publish and not receive patent	Publicly use the invention more than a year before filing for patent  Sell or offer to sell the invention more than one year before filing for patent  Otherwise permit your own work to become prior art to your patent application  Make an insufficient disclosure to the Patent Office in the patent application or during prosecution of the application  Fail to have invention assignment agreement with key employees

## Chapter 3

# Keeping Trade Secret Information Secret

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

In evaluating whether a party has taken reasonable precautions, courts typically consider several factors, including whether there is a written confidentiality agreement restricting disclosure. The absence of a written confidentiality agreement is not fatal to a trade secret claim but it does make it harder for a company claiming trade secret protection to prove its case. Courts also consider: the nature and extent of security precautions to protect the information; whether the circumstances of the disclosure (either to an employee or to a third party) give rise to a reasonable inference that further disclosure without consent is prohibited; and the degree to which the information has been placed in the public domain or rendered “readily ascertainable” by third parties, for example through patent applications or marketing. Of course, voluntary disclosure to third parties without appropriate agreement as to the trade secret nature of the information may mean the information is not a protectable trade secret.

A critical part of security can be defining the company’s trade secrets proactively. Instead, one of the most common scenarios

(and one of the most common problems in litigation) is that until someone becomes concerned a trade secret has been misappropriated, nobody has defined what are a company's trade secrets. Once a company is concerned misappropriation has occurred, it can be overbroad about what it believes 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, partners, or other businesses specifying that the information is trade secret as well as the legitimate uses of the information
- Written non-competition agreements with employees or other business partners
- Granting access to information on a need-to-know basis
- Preventing unauthorized access to information (e.g., keeping information in locked rooms or cabinets, restricting access to locations where information is stored, putting password restrictions on computer files)
- Sign in/sign out procedures
- Educating employees on the company's trade secret policies
- Marking documents that contain trade secret information as confidential
- Implementing a computer security policy (e.g., limiting access to information stored on off-site computers)
- Ensuring that sales employees do not reveal trade secrets in the process of marketing products

By taking these and other precautions, owners get two valuable benefits. First, owners are able to exercise more control over their information. Second, if someone does wrongfully take the information, it will be easier to seek court protection and remedies.

### Case Studies

Two recent 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 Kodak's 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 prevent Kodak from appropriating its information.

## Employee Agreements: Non-Disclosure and Non-Competition Agreements

Two types of agreements with employees to protect trade secrets deserve special attention: non-disclosure 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.

Non-disclosure agreements are useful when a party holding confidential information, such as a trade secret, wants to disclose it to a third party without risking that it be disclosed to anyone else. In one common situation, this occurs when an employer hires an employee and wants to ensure that the employee will not share the employer's trade secrets with others during or after employment. An effective non-disclosure agreement should define the confidential information, the exclusions to what is confidential information, the obligations of the employee to hold the information confidentially, and the time period for which the confidentiality of the information must be maintained. Information disclosed without such an agreement risks losing its trade secret status.

To enhance the effectiveness of a non-disclosure agreement, it is helpful to hold an exit interview when an employee leaves the company. At the least, the meeting is an opportunity to remind the employee of any obligations under the agreement. Such an interview can also lay the foundation to later prove a violation of the non-disclosure agreement. For example, if the employee lies about plans for future employment or recent computer activity, the employer has secured powerful evidence that the employee is violating the non-compete agreement.



Non-disclosure agreements do not prevent an employee from becoming or working for a competitor, however. For that, you need a non-competition agreement. For a non-compete agreement to hold up in court, it must be reasonable. First, there should be good business reasons for the agreement. Punishing an employee for leaving the company will not pass muster as a valid reason for a non-compete, but having one for the purpose of protecting trade secrets will. Second, the employee must receive consideration - a benefit such as an offer of employment or a raise - in exchange for the restriction. Third, the restriction also should 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 the agreement is reasonable for protecting the trade secret owner's information, not to create hardship on the employee. Still, some jurisdictions, such as California, will not enforce a non-competition agreement except in limited circumstances (e.g., the sale of a business).

## Chapter 4

# What Is Trade Secret Misappropriation?

### Misappropriation Defined

The Uniform Trade Secrets Act defines misappropriation broadly to include the *acquisition* of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means. It also includes the *disclosure or use* of someone else's trade secret without express or implied consent by a person who:

- 1) used improper means to learn the trade secret; *or*
- 2) knew or had reason to know that his or her knowledge of the trade secret was:
  - (a) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; *or*
  - (b) derived from a person who used improper means to acquire it; *or*
  - (c) derived from a person who owed a duty to the party claiming trade secret protection to maintain its secrecy; *or*
- 3) before a material change in position, knew or had reason to know that the information was a trade secret and that knowledge of it had been acquired by accident or mistake.

Misappropriation usually occurs by two different types of actors: those who are in a special relationship with the trade secret owner (such as an employee, customer, or vendor) and strangers. A very common scenario in a lawsuit involving claims of trade secret misappropriation is that an employee leaves one company to

start or work for a competitor. The old employer may fear that the former employee will use information acquired during work for the old employer in the new job. Other common scenarios are when two companies work together, either in a customer/vendor relationship or as collaborators in research and/or product development. Old fashion theft can also occur.

### **What Is Not Misappropriation**

The law allows discovery of a trade secret by proper means. Proper means include:

- A license from the trade secret owner; *or*
- Discovery by independent effort; *or*
- Learning the trade secret from published literature; *or*
- Observation of the item in public use or on public display; *or*
- Freedom of Information Act requests for information provided by competitors to the government without proper protection for trade secrets; *or*
- Reverse engineering – that is starting with the competitor product and working backwards to learn how it was developed.

Much of trade secret litigation can focus on whether the alleged wrongdoer could have or did properly discover the claimed trade secret.

## Chapter 5

# Remedies for Trade Secret Misappropriation

Two kinds of relief are available for actual or threatened trade secret misappropriation. A court may grant an *injunction* (i.e., a court order) that protects the trade secret owner and prevents the misappropriator from using the secret information. In addition, the court may 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.

### Injunctive Relief

A court may order a party not to use information subject to trade secret protection under certain circumstances. A court may issue an injunction to prevent:

- Additional harm to the trade secret owner or to prevent the misappropriator from continuing to benefit from the trade secret;
- The misappropriator from getting an unfair head start even when the information is no longer secret; *or*
- The misappropriator from disclosing the trade secret to others.

The UTSA also provides that in exceptional circumstances, a court may issue an injunction conditioned on payment of a reasonable royalty for no longer than the period of time for which use could have been prohibited. Exceptional circumstances include when a complete bar to use would be inequitable, for example, where a party made a material and prejudicial change of position prior to acquiring knowledge or reason to know of the misappropriation.

Another key issue with injunctions is the length. Courts may enter a permanent injunction, with the burden on the accused party to seek an end to the injunction upon a showing that the trade secret is no longer a trade secret. A court might also determine at the outset how long the injunction should be to remedy the harm caused by the misappropriation. For example, someone accused of misappropriation might argue the injunction should last no longer than the time it would have taken to independently develop the trade secret. When that period is hard to determine, courts tend to err on the side of the trade secret owner.

### Examples:

- Company B misappropriates Company A's secret assembly-line layout. A court could prevent Company B from using the secret layout.
- Company A has a secret process of removing impurities from the syrup it produces. Company B is developing a similar process, but, to save the six-month development time, misappropriates Company A's trade secret. A court could prevent Company B from using Company A's trade secret for six months.
- Salesperson X, an employee of Company A, misappropriates Company A's customer list by taking a copy with him after he quits. A court could order Salesperson X to return the list (and any copies), and order Salesperson X not to use the list at his new company.

## 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 as a result of the wrongdoing
- 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

In some states, punitive or exemplary damages may be available to further punish the misappropriator. Depending on the circumstances and state law, compensation for attorneys' fees may also be available.

## Chapter 6

# Criminal Enforcement of Trade Secrets

Although companies have less control over the criminal justice process than they do over private litigation, criminal laws can provide one or more additional tools to help trade secret owners protect their rights. In addition to state laws providing trade secret protection, including criminal penalties, two federal laws in particular may help protect trade secret owners: the [Economic Espionage Act](#), 18 U.S.C. § 1831 – 1839, and the [Computer Fraud and Abuse Act](#), 18 U.S.C. § 1030.

### Economic Espionage Act

The Economic Espionage Act (EEA) makes it a federal crime to misappropriate trade secrets and provides protection against both domestic and foreign conduct. The EEA criminalizes misappropriation of trade secrets in two main areas based upon who benefits from the conduct. Section 1831 criminalizes conduct that will benefit a foreign government, foreign entity, or agent of either. Section 1832 criminalizes trade secret misappropriation for the economic benefit of anyone other than the owner, provided the misappropriation is related to a product placed in interstate or international commerce.

A trade secret is broadly defined under the EEA 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, the public[.]”

The EEA criminalizes conduct by anyone who knowingly:

- 1) Steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;
- 2) Without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret; or
- 3) Receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization. Attempt and conspiracy to commit these offenses are also criminalized.

The U.S. Attorney General also has the authority to obtain injunctive relief through a civil action against a violation of the EEA. Individuals or corporations, however, have no private right of action to obtain injunctive relief under the EEA. They are the victim in a government criminal prosecution. Penalties for violation of the EEA include



imprisonment, fines of up to \$500,000 for an individual, and forfeiture of property.

### **Computer Fraud and Abuse Act**

The Computer Fraud and Abuse Act (CFAA) provides another federal means for protecting trade secret rights by criminalizing certain activity where a computer is used.

As it can be applied to trade secret information, the CFAA makes it a crime to intentionally access a computer without authorization or exceed authorized access and obtain information from any protected computer (a computer used in interstate or foreign commerce or communication) if the conduct involved an interstate or foreign communication. The CFAA also makes it a crime to intentionally access a protected computer without authorization and cause damage or loss. Since computers are used everywhere in business today, with a substantial portion connected to the Internet, the CFAA covers most computers.

Notably, the CFAA places no restriction on what constitutes “information.” Therefore, the sometimes difficult issue of proving the existence of a trade secret does not arise. Damage includes any impairment to the integrity of information, and this has been interpreted to include conduct that compromises the secret nature of information.

Those acting without authorization typically are outsiders, such as a computer hacker, whereas those exceeding authorized access typically addresses insiders, or employees, who may already have some limited computer privileges but who exceeded that authorization.

The CFAA provides for both criminal and civil remedies. Criminal punishment can vary widely and reach as high as 20 years, depending on which provision of the CFAA was violated and whether the violation was a repeat offense. Where a party has suffered damage or loss, the CFAA allows a party to pursue a civil action in federal court with certain restrictions.

## Chapter 7

# The Flip Side of Trade Secrets: How Not to Misappropriate

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

- Screening incoming employees for confidentiality 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

As with protecting trade secrets, an ounce of prevention is worth a pound of cure. 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. Companies that take advantage of trade secret protections have a significantly better likelihood of keeping their proprietary information secure. When used correctly, trade secret protections can protect some information indefinitely. 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 LLP is a leading national law firm in the areas of dispute resolution, intellectual property, and corporate transactions for emerging, middle-market, and large-cap companies. With a deep understanding of clients' strategic priorities, operational imperatives, and marketplace realities, the firm helps companies in the biopharma, high technology, energy technology, financial services and manufacturing sectors gain competitive advantage. The firm's 225 lawyers located in Boston, Washington, and the Emerging Enterprise Center in Waltham, Massachusetts join with a network of Lex Mundi law firms to provide global support for clients' largest challenges and opportunities. For more information visit [foleyhoag.com](http://foleyhoag.com).

## Vickie L. Henry

Vickie Henry has focused her 15-year litigation career on resolving intellectual property and product liability disputes, with her work in these areas based on a solid background in general commercial litigation. She has tried more than 20 trials to verdict or judgment.

The intellectual property matters that Vickie handles involve both patent litigation and analysis and litigation of trade secrets. She has represented corporate and individual clients as both plaintiffs and defendants in these matters. Her clients come from a diverse range of businesses and industries, including pharmaceuticals, medical devices, telecommunications and food processing equipment. Vickie's product liability work shows a similar wide range of experience, from pharmaceutical and medical device liability to toxic tort cases to consumer product liability. She has tried these matters throughout the country in state and federal courts at both the trial and appellate levels.

Click the image below for a full biography.



Vickie L. Henry

## Claire Laporte

Claire Laporte has received recognition in both Chambers USA and Massachusetts SuperLawyers for her extensive and successful intellectual property practice. She represents clients in complex patent litigation and technology-related matters in a broad range of technical specialties including biotechnology, medical devices, pharmaceuticals, e-commerce, computer vision, and other software. Claire's litigation focus is in the federal courts, but she has also provided clients with representation before the International Trade Commission. In addition to her trial practice, Claire undertakes extensive appellate work, both in client representation and the filing of amicus briefs with the U.S. Supreme Court and the Federal Circuit Court of Appeals.


Click the image below for a full biography.

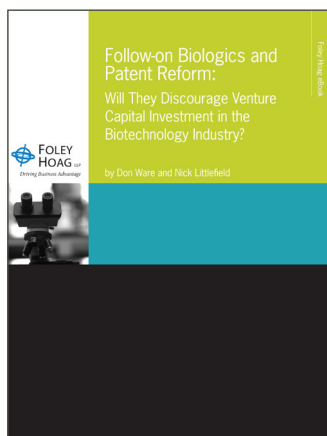
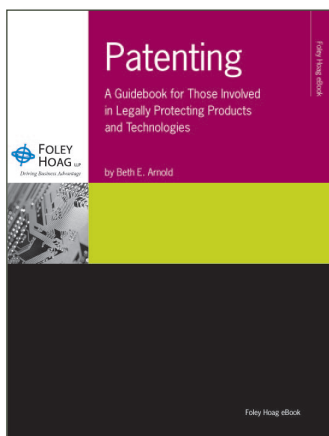


*Claire Laporte*

## Foley Hoag eBook Library

Sample other free titles from the Foley Hoag eBook library, sign-up for industry-specific alerts and updates from Foley Hoag, or visit our Web site.

Visit our Web site  Sign up for industry-specific alerts and updates



You may also be interested in our eBook series. Simply click on an image to download or visit [foleyhoag.com](http://foleyhoag.com) for our library.

TRADE SECRETS



617 832 1000 *tel* 617 382 7000 *fax*

BOSTON | WASHINGTON | EMERGING ENTERPRISE CENTER | FOLEYHOAG.COM