Trade Secrets

Alternative to Patent Protection

Paul F. Neils
Jean C. Edwards

What are Trade Secrets?

- Trade secret law developed from state common and statutory laws, and aims to avoid misappropriation of valuable business information.
- There are currently three major statutes which relate to the misappropriation of trade secrets:
  - the Uniform Trade Secrets Act;
  - the Economic Espionage Act;
  - and the Computer Fraud and Abuse Act.
- There is currently no federal civil cause of action for trade secret misappropriation in the U.S.
  - The only possible federal action is criminal prosecution by the Dept. of Justice through action by a U.S. Attorney—however, this is rarely used.

What are Trade Secrets? (contd.)

- The Restatement (Third) of Unfair Competition, the Restatement of Torts, the Uniform Trade Secrets Act and several other acts all have varying definitions of a trade secret.
- Definitions of "trade secret," typically have three common characteristics—information that:
  - ✓ is not generally known to the public;
  - ✓ confers some sort of economic benefit on its holder; and
  - ✓ is the subject of reasonable efforts to maintain its secrecy.
- Most statues also have unique characterizations of what constitutes the misappropriation or theft of trade secrets.

What are Trade Secrets? (contd.)

- No exclusive rights exist in a trade secret – the owner of a trade secret has no recourse if a third party independently invents the information, discovers the information through reverse engineering, or obtains the information due to accidental disclosure.
  - These are the traditional common law defenses to trade secret misappropriation.
- In addition to statutes that protect trade secrets, a company often protects its confidential proprietary information through non-compete and non-disclosure contracts with its employees.

Protecting Trade Secrets

- Uniform Trade Secrets Act
- Economic Espionage Act
  18 USC § § 1831-1839
- Computer Fraud and Abuse Act
  18 USC § 1030

Uniform Trade Secrets Act

- The Uniform Trade Secrets Act (UTSA) is a model law drafted by the National Conference of Commissioners on Uniform State Laws in 1974.
- The goal of the UTSA was to better define the rights and remedies of common law trade secret.
- The UTSA has been adopted by 46 states, the District of Columbia and the U.S. Virgin Islands.
- Massachusetts, New Jersey, New York, and Texas have yet to adopt the USTA. Some of these states still apply common law to trade secrets, have adopted separate state statutes, or draw guidance from the Restatement of Torts.
- In 2010, the UTSA was introduced in the Massachusetts, New York and New Jersey legislatures.

Uniform Trade Secrets Act (contd.)

- The UTSA defines a "trade secret" as:
  - "Information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
    - 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
    - It is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

Uniform Trade Secrets Act (contd.)

- Misappropriation Under the UTSA
  - Misappropriation is the wrongful acquisition, disclosure or use of a trade secret
    - Includes acquiring the secret through improper means or from another person knowing that they acquired the secret by improper means or disclosing the secret without consent when circumstances create a duty not to disclose or use it.
    - Can also include accidental or mistaken acquisition of a trade secret, if before using or disclosing the trade secret, the person acquiring it learns that it is a trade secret.

Remedies for Trade Secret Misappropriation

- The UTSA creates a private right of action for the victim of trade secret misappropriation and imposes civil, rather than criminal, liability for misappropriation of trade secrets.
- Possible remedies include injunctions, compensatory and punitive damages.

Remedies for Trade Secret Misappropriation (contd.)

- Injunctive relief is available to prevent trade secret misappropriation, whether it be actual or threatened. UTSA § 2.
  - A trade secret owner can file for a preliminary injunction upon discovering that a third party has misappropriated the secret information
  - May be costly, but can prevent infringers from continued violation of the trade secret pending the resolution of the litigation.

Remedies for Trade Secret Misappropriation (contd.)

- Maintaining secrecy during litigation
  - According to UTSA § 5, a court shall preserve the secrecy of an alleged trade secret by reasonable means, which may include:
    - granting protective orders in connection with discovery proceedings;
    - holding in-camera hearings;
    - sealing the records of the action; and
    - ordering any person involved in the litigation not to disclose an alleged trade secret without prior court approval.

Remedies for Trade Secret Misappropriation (contd.)

- Under the UTSA, damages for misappropriation of a trade secret can include both the actual loss caused by the misappropriation and the unjust enrichment caused by the misappropriation that is not taken into account in computing the actual loss. UTSA § 3(a).
- In addition, the right to a reasonable royalty can also be used as a remedy for trade secret misappropriation if the actual loss or unjust enrichment cannot be proved by a preponderance of the evidence. UTSA § 3(a).

Remedies for Trade Secret Misappropriation (contd.)

- In the event of willful and malicious misappropriation of a trade secret, the court may award exemplary (punitive) damages in the amount not exceeding twice the amount of compensatory damages. UTSA § 3(b).
- In the case of bad faith or willful and malicious misappropriation, reasonable attorney's fees may be awarded.

Remedies for Trade Secret Misappropriation (contd.)

- A court may award reasonable attorney's fees to the prevailing party if:
  i. a claim of misappropriation is made in bad faith;
  ii. a motion to terminate an injunction is made or resisted in bad faith, or
  iii. willful and malicious misappropriation exists.

UTSA § 4.

Uniform Trade Secrets Act (contd.)

- Defenses under the UTSA
  - Defenses traditionally recognized in common law, such as disclosure by the owner, reverse engineering and independent development – are not codified in the UTSA.
- Criticism of the UTSA
  - Even with the UTSA, there is a lack of uniformity in state trade secret laws - states still vary widely in their treatment of trade secret misappropriation.
  - For example, trade secret cases in different states are subject to different procedural rules.

Uniform Trade Secrets Act (contd.)

- The UTSA permits courts to grant protective orders to maintain the secrecy of a trade secret during discovery, however, disclosure to a defendant may be necessary.

Trade Secrets v. Patents

- A patent is a grant from the federal government to the recipient (referred to as "the patentee") of the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States or importing the invention into the United States.
- A patent does not give the patentee the right to make, use, etc., his invention in the United States.
- Thus, the exclusive right to exclude others from making, using, etc., for a limited time is regarded as a *quid pro quo* for disclosing the information to the public.

Trade Secrets v. Patents (contd.)

- Utility patents are granted for new and useful inventions or discoveries directed to processes, machines, manufactures, or compositions of matter, or any new and useful improvements of any of these listed items.
- A utility patent has a term of 20 years from the earliest filing date of the U.S. application for patent, or, if the utility patent is based on a continuing application which claims benefit from an earlier filed parent U.S. application, 20 years from the filing date of the earliest filed parent U.S. application.

Trade Secrets v. Patents (contd.)

- Like patents, trade secrets protect information.
- However, the life of a trade secret is not fixed and depends on whether it is kept secret.
- Public disclosure of a trade secret ends the life of it.
- Unlike patents, trade secret protection extends only with respect to confidential relationships and does not prevent independent discovery by another.

Trade Secrets v. Patents (contd.)

- Independent development or discovery may be lawfully accomplished by, for example, reverse engineering a product or process.
- The most famous example of a trade secret is the formula for Coca Cola®.
- Despite much effort on the part of Coke's® competitors, no one has been able to reverse engineer the formula for Coke® for over 100 years.

Creating A Trade Secret

- There should be a written agreement between the owner of the trade secret and any individual or company (e.g., a contractor) who has access to the trade secret.
- The written agreement must be marked as "Confidential," "Proprietary," "Secret," or the like.

Creating A Trade Secret (contd.)

- The written agreement should clearly set forth the limits and restrictions of the trade secret.
- Written agreements can take the form of:
  - non-disclosure agreements (NDAs);
  - non-compete clauses;
  - employment agreements; and
  - other agreements accomplishing similar objectives.

Creating A Trade Secret (contd.)

- Companies that develop intellectual property (IP) normally require their employees, as a condition of employment, to sign an employment agreement or contract which requires that all IP be assigned to the company for all work done by the employee.
- Some companies will not require that IP developed by an employee outside the scope of employment and after hours or weekends be owned by the company.

Creating A Trade Secret (contd.)

- It is important to note that if a company hires an independent contractor to create IP, the independent contractor owns the IP unless the contract specifically spells out that all IP when created in connection with the contract must be assigned to the company.
- Moreover, in contracts, such as employment contracts, every word matters.

Case Law

- ***Mattel Inc. v. MGA Entertainment Inc.***, No. 09-55673 (9th Cir. July 22, 2010)
  - Involved the rights to the Bratz dolls, developed by a former employee of Mattel, Carter Bryant, who worked on Barbie designs and styles.
  - Carter agreed in his employment contract to assign "all inventions" that he developed to Mattel while employed by the company.
  - However, the issue in the case was whether this term unambiguously covered *ideas*, such as Bryant's concept for the pouty, heavily made-up Bratz dolls, which he later took to Mattel's competitor MGA Entertainment Inc.
  - In the case, the Ninth Circuit noted that *ideas* were markedly different from the examples of inventions included in the contract, such as "designs, know-how, data computer programs and formulae."

Case Law (contd.)

- The *Mattel v. MGA Entertainment* ruling illustrates the need to carefully choose your words when drafting agreements with provisions designed to protect your IP, such as the employment contracts at issue in the case.
- Terms like "inventions" may be fine in industries where the IP relates to articles of manufacture that may be patentable, whereas the term "ideas" may be better with items or concepts that are less likely to be patentable.

Why Rely on Trade Secrets?

- A new idea, innovation, or invention may be unpatentable because it does not meet the legal requirements for patentability (i.e., usefulness, novelty, and non-obviousness).
- Before a patent is obtained or applied for, an inventor may want to disclose it to a prospective financial backer, manufacturer, or the like.
- Secrecy may be preferable over the great expense of patent prosecution and/or litigation, especially if any patent obtained is extremely narrow in scope or of questionable validity.

Why Rely on Trade Secrets? (contd.)

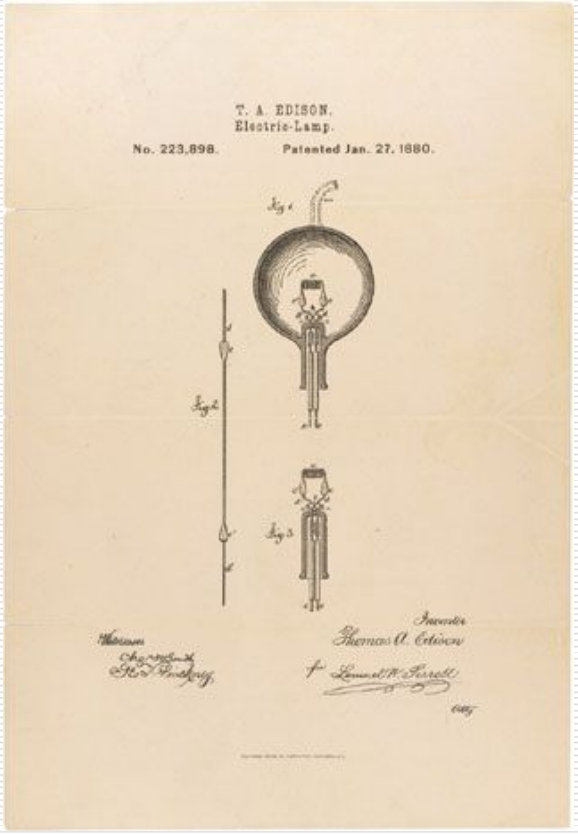
- Regarding secrecy, keep in mind that the inventor can file a Request for Non-Publication at the time of filing a patent application in the U.S., as long as he does not intend to foreign file the patent application.
- This will keep the application secret in the patent office should the inventor ultimately decide to abandon the patent application, thus preserving the trade secret as long as no other public disclosure has been made.
- If the inventor also wants to obtain patent protection in other countries, he cannot file such a Non-Publication Request, as the patent laws require publication of the application.
  - See 35 U.S.C. § 122 (b)(1)(A).

Why Rely on Trade Secrets? (contd.)

- Of course, in the absence of a Non-Publication Request, the patent application will be published by the U.S. Patent & Trademark Office (USPTO) approximately 18 months from the filing date of the patent application, thus ending any possible trade secret protection.
- Also, if a patent application which has been published is ultimately determined to be unpatentable by the USPTO and abandoned by the applicant, the applicant/inventor has lost both patent protection and trade secret protection in view of the public disclosure.

Other Advantages of Trade Secrets

- **Negative know-how can be protected by trade secret.**
- Example: Thomas Edison is said to have failed 10,000 times before discovering how to make the filament in the light bulb become incandescent without burning up or melting after a short period of time when heated by an electric current.
  - Edison is credited with inventing the first practical incandescent bulb, which used a carbonized Japanese bamboo thread as the filament.
  - This information of 10,000 "failures" or things that did not work was a valuable trade secret that would be very important to protect from Edison's competitors.


T. A. EDISON.
Electric-Lamp.
No. 223,898. Patented Jan. 27, 1880.

Maintaining Secrecy of Trade Secrets

- Trade secrets can be misappropriated by:
  - A breach of a duty of confidentiality (an issue that arises frequently in the case of departing employees); or
  - Engagement of other improper means (does not have to be illegal per se) to steal a trade secret, i.e., information theft, commercial espionage.

Maintaining Secrecy of Trade Secrets (contd.)

- According to the UTSA, "improper means" includes (i.e., not an exclusive list):
  - theft;
  - bribery;
  - misrepresentation;
  - breach or inducement of a breach of a duty to maintain secrecy;
  - or espionage through electronic or other means

Maintaining Secrecy of Trade Secrets (contd.)

- The UTSA only protects a secret that is "...subject of efforts that are reasonable under the circumstances to maintain its secrecy"
- What constitutes "reasonable efforts"?
  - For each particular circumstance, the procedures and safeguards to protect the trade secret will be a bit different.
  - The size and sophistication of an individual company and industry are considered.
  - E.g., employment contracts, confidentiality agreements, internal compliance rules, reasonable security measures, etc.

Maintaining Secrecy of Trade Secrets (contd.)

- Perfect security is not necessarily optimum security.
  - Spending more money on security means demonstrates that the trade secret is more valuable; but
  - More security could mean that conducting your day-to-day business is much more difficult.
- Oral confidentiality agreement could suffice for a small business, but agreement should be put in writing if possible.
  - Implied or oral contracts are much more difficult to enforce or prove.

Maintaining Secrecy of Trade Secrets (contd.)

- Employer—Employee Relationships
  - Non-compete agreements seek to prevent an employee from entering into competition with the employer for a period of time and within a particular geographic area.
  - Non-compete agreement must be reasonable in time and scope.
  - Employee is free to use his general knowledge or skill for his own benefit or the benefit of others.

Maintaining Secrecy of Trade Secrets (contd.)

- **Doctrine of Inevitable Disclosure**: used when an employee may inevitably disclose his former employer's trade secrets even though it is not his intention.
  - Plaintiff can seek to enjoin a defendant from working for his new employer in a particular capacity.
  - Most jurisdictions recognize this doctrine, but others, such as California, do not.
  - Consider Factors:
    - Circumstances surrounding the termination of employment;
    - Importance of employee's job or position;
    - Type of work performed by the employee; and
    - Type of information sought to be protected and the value of the information or the competitor's need for it.

Maintaining Secrecy of Trade Secrets

- Trade secrets can be time-dependent:
  - A trade secret business plan may be very valuable today, but often has decreasing value with time.
  - There may be a time in the future when the information an employee takes with him, although once considered a trade secret, is no longer considered a trade secret.

Proving Trade Secret Misappropriation

- Restatement (First) of Torts – factors to consider to determine whether a secret exists:
  - Extent to which the information is known outside the business;
  - Extent to which the information is known by employees and others involved in the business;
  - Extent of measures taken to guard the secrecy of information;
  - Value of information to business and competitors;
  - Amount of time, effort, and money expended in developing the information;
  - Ease or difficulty with which the information could be properly acquired or duplicated by others.

Proving Trade Secret Misappropriation

- Proof of misappropriation can be based on circumstantial evidence:
  - Access plus substantial similarity or substantial derivation is sufficient.
  - Does not require a showing that all elements have been copied.

More Case Law

- ***E.I. Dupont v. Christopher***, 431 F. 2d 1012 (5th Cir. 1970): From a plane, defendant took aerial photos of the plaintiff's plant during construction. This was not illegal per se. Plaintiff successfully sued for misappropriation of a trade secret.
  - "Improper means of discovery" are defined in the Restatement of Torts:
    - Means which fall below the generally accepted standards of commercial morality and reasonable conduct.
    - E.g., fraudulent misrepresentations, tapping of phone wires, eavesdropping, other espionage.
  - Trade secret holder is not required to guard against the unanticipated, undetectable, or unpreventable methods of espionage.
  - Persons or corporations are not required to take "unreasonable precautions" to prevent another from doing "that which he ought not do in the first place."

More Case Law (contd.)

- ***Pepsico v. Redmond***, 54 F.3d 1262 (7th Cir. 1995): Pepsi sought a preliminary injunction to prevent a former employee from divulging trade secrets and confidential information (related to beverage pricing, marketing and distribution) to Quaker, his new company.
  - Threatened misappropriation can be enjoined where there is a high degree of probability of inevitable and immediate use of trade secrets.
  - Does not apply to "general skills and knowledge" acquired during tenure with the plaintiff's company, but rather "the particularized plans or processes developed by the plaintiff and disclosed to him while the employer-employee relationship existed, which are unknown to others in the industry and which give the employer an advantage over its competitors."

Defenses to Trade Secret Misappropriation

- Improper means were not used in acquiring information:
  - Reverse engineering (not improper means);
  - Independent creation (not improper means);
- No duty of confidentiality or agreement existed (or no breach was made);
- The information was not secret—known in the industry;
- The information did not have commercial value or was of nominal value.

Considering Trade Secret Protection

- Considerations in favor of protecting IP through trade secret:
  - The patentability of the IP is questionable and the owner does not want to risk disclosure through USPTO publication.
  - A patent covering the IP would be narrow and provide competitors with ample ability to design-around the IP.
  - The IP owner does not want to undertake the costs of patent prosecution or foresees a long prosecution battle.
  - Reverse engineering will be difficult or costly for competitors to accomplish.
  - The nature of the information is such that it will not be too difficult to prove misappropriation.

Protecting Trade Secrets: Economic Espionage Act

- In 1996, the United States enacted the Economic Espionage Act (EEA), making the theft or misappropriation of a trade secret a federal crime.
- Unlike what is traditionally considered espionage, this Act covers commercial information, not classified or national defense information.
- The difference between the definition of trade secret under the EEA and the UTSA is that under the EEA, information is a trade secret if it is not generally known to competitors and the general public.

Economic Espionage Act (contd.)

- Under the EEA, trade secret is broadly defined as: "[A]ll 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 –
  - the owner thereof has taken reasonable measures to keep such information secret; and
  - 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." 18 USC § 1839(3)

Economic Espionage Act (contd.)

- The EEA covers two distinct kinds of trade secret misappropriation.
- § 1831 of the EEA criminalizes the misappropriation of trade secrets with the knowledge or intent that the theft will benefit a foreign power.
  - Penalties for violation of this section include fines of up to $500,000 per offense and imprisonment for up to 15 years.
  - If an organization or corporation is involved in the misappropriation, fines of up to $10 million are possible.

Economic Espionage Act (contd.)

- § 1832 involves misappropriation of trade secrets related to or included in a product in interstate commerce with the knowledge or intent that the misappropriation will injure the owner of a trade secret.
- Penalties for violation of this section include imprisonment for up to 10 years for individuals and fines of up to $5 million for organizations.
- Unlike the penalties under Section 1831, there is no fine for individuals who misappropriate a trade secret under Section 1832.

Economic Espionage Act (contd.)

- In addition to the penalties set for in § § 1831 and 1832, Section 1834 of the EEA requires criminal forfeiture of:
  - Any proceeds of the misappropriation or attempted misappropriation and any property derived from the crime; as well as
  - Any property used in the commission or attempted commission of the crime.

Economic Espionage Act (contd.)

- Misappropriation Under the EEA
  - Misappropriation or theft of trade secrets includes:
    - Stealing protected information;
    - Obtaining such information by fraud or deception;
    - Copying, duplication, photographing, downloading, sending, mailing or destroying such information;
    - Receiving, buying, possessing such information or knowing it to have been stolen or obtained without authorization; and
    - Conspiring with one or more other person to do any of the above.

Economic Espionage Act (contd.)

- Remedies Under the EEA
  - While the EEA authorizes civil proceedings by the Department of Justice, it does not create a private right of action.
  - The only remedy available to victims of trade secret misappropriation is injunctive relief.

Economic Espionage Act (contd.)

- **Criticism of the EEA:**
  - Many consider this to be poorly drafted legislation. Because government attorneys prefer not to test bad legislation, the EEA has only been used in a handful of cases.
  - The U.S. Attorney has a high burden – must prove beyond a reasonable doubt that the defendant acted with specific intent; defendant attempted or conspired to convert the trade secret for the economic benefit of someone other than owner; and defendant intended to injure the owner of the trade secret.
  - This high requirement seems to narrow the scope of EEA prosecutions to only clear cases of theft of tangible property where there is physical evidence of the misappropriation.

Economic Espionage Act

- **Criticism of the EEA (contd.):**
  - Pursuing relief through the EEA may compel the disclosure of formerly confidential proprietary information to the defendant as part of the criminal case, essentially forcing a victim corporation to reveal the trade secrets the corporation was seeking to protect.
  - Civil statutes and common law theories may offer vicitims more protection than the EEA because of the potential to obtain compensatory damages, although victims may still be compelled to disclose trade secrets during proceedings.
  - The requirement that the product be in interstate commerce to be protected by the EEA could be problematic when the product at issue is still in the research and development phase.

Protecting Trade Secrets: Computer Fraud and Abuse Act

- The Computer Fraud and Abuse Act (CFAA) was originally enacted to protect classified information and financial records contained in computers of governmental and financial institutions.
- After several revisions, the CFAA has been expanded to cover "protected computers," which simply means any computer connected to the internet.
- Only recently, the CFAA has been applied to provide a potential remedy for conduct involving the misappropriation of trade secrets.

Computer Fraud and Abuse Act

- *Shurgard Storage Centers v. Safeguard Self Storage,* 119 F Supp 2d 1121 (W.D. Wash. 2000) was one of the first reported cases to apply the CFAA to misappropriation of trade secrets.
- To bring a civil claim under the CFAA, a party must:
  1. establish at least one category of misconduct set forth in the Act; and
  2. satisfy the "damage or loss" requirement.
- Under the Act, the following misconduct is relevant to trade secrets:
  - Theft of computer data;
  - Unauthorized Access with the Intent to Defraud;
  - Unauthorized Access Resulting in Damage to Computer;
  - Trafficking in Computer Passwords;
  - Extortion by Threat of Damage to Computer.

Computer Fraud and Abuse Act (contd.)

- Under the CFAA, a plaintiff must plead and prove damage or loss of at least $5,000 attributable to the alleged violation of the Act.
- Criticism of the CFAA:
  - The CFAA is primarily aimed at computer crimes, and as such the scope of protection for trade secrets is unclear.

Additional Information about Trade Secrets

- Some believe the United States is not in compliance with the NAFTA and TRIPs Agreements, which require national standards for trade secret protection, since some states still rely on common law when dealing with trade secret misappropriation.

Closing

Q & A