

18.3: Trade Secrets

Learning Objectives

By the end of this section, you will be able to:

- Describe the difference between trade secrets and patents, and explain why a firm might prefer keeping a trade secret rather than obtaining a patent.
- Understand the dimensions of corporate espionage and the impact of the federal Economic Espionage Act.

Definition of Trade Secrets

A patent is an invention publicly disclosed in return for a monopoly. A trade secret is a means to a monopoly that a company hopes to maintain by preventing public disclosure. Why not always take out a patent? There are several reasons. The trade secret might be one that is not patentable, such as a customer list or an improvement that does not meet the tests of novelty or nonobviousness. A patent can be designed around; but if the trade secret is kept, its owner will be the exclusive user of it. Patents are expensive to obtain, and the process is extremely time consuming. Patent protection expires in twenty years, after which anyone is free to use the invention, but a trade secret can be maintained for as long as the secret is kept.

However, a trade secret is valuable only so long as it is kept secret. Once it is publicly revealed, by whatever means, anyone is free to use it. The critical distinction between a patent and a trade secret is this: a patent gives its owner the right to enjoin anyone who infringes it from making use of it, whereas a trade secret gives its “owner” the right to sue only the person who improperly took it or revealed it.

According to the Restatement of Torts, Section 757, Comment b, a trade secret may consist of any formula, pattern, device or compilation of information which is used in one’s business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it. It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers....A trade secret is a process or device for continuous use in the operation of a business. Generally it relates to the production of goods, as, for example, a machine or formula for the production of an article.

Other types of trade secrets are customer information, pricing data, marketing methods, sources of supply, and secret technical know-how.

Elements of Trade Secrets

To be entitled to protection, a trade secret must be (1) original and (2) secret.

Originality

The trade secret must have a certain degree of originality, although not as much as would be necessary to secure a patent. For example, a principle or technique that is common knowledge does not become a protectable trade secret merely because a particular company taught it to one of its employees who now wants to leave to work for a competitor.

Secrecy

Some types of information are obviously secret, like the chemical formula that is jealously guarded through an elaborate security system within the company. But other kinds of information might not be secret, even though essential to a company’s business. For instance, a list of suppliers that can be devised easily by reading through the telephone directory is not secret. Nor is a method secret simply because someone develops and uses it, if no steps are taken to guard it. A company that circulates a product description in its catalog may not claim a trade secret in the design of the product if the description permits someone to do “reverse engineering.” A company that hopes to keep its processes and designs secret should affirmatively attempt to do so—for example, by requiring employees to sign a nondisclosure agreement covering the corporate trade secrets with which they work. However, a company need not go to every extreme to guard a trade secret.

Trade-secrets espionage has become a big business. To protect industrial secrets, US corporations spend billions on security arrangements. The line between competitive intelligence gathering and espionage can sometimes be difficult to draw. The problem

is by no means confined to the United States; companies and nations all over the world have become concerned about theft of trade secrets to gain competitive advantage, and foreign governments are widely believed to be involved in espionage and cyberattacks.

Economic Espionage Act

The Economic Espionage Act (EEA) of 1996 makes the theft or misappropriation of a trade secret a federal crime. The act is aimed at protecting commercial information rather than classified national defense information. Two sorts of activities are criminalized. The first section of the act Economic Espionage Act, 18 United States Code, Section 1831(a) (1996) criminalizes the misappropriation of trade secrets (including conspiracy to misappropriate trade secrets and the subsequent acquisition of such misappropriated trade secrets) with the knowledge or intent that the theft will benefit a foreign power. Penalties for violation are fines of up to US\$500,000 per offense and imprisonment of up to fifteen years for individuals, and fines of up to US\$10 million for organizations.

The second section Economic Espionage Act, 18 United States Code, Section 1832 (1996). criminalizes the misappropriation of trade secrets related to or included in a product that is produced for or placed in interstate (including international) commerce, with the knowledge or intent that the misappropriation will injure the owner of the trade secret. Penalties for violation are imprisonment for up to ten years for individuals (no fines) and fines of up to US\$5 million for organizations.

In addition to these specific penalties, the fourth section of the EEA Economic Espionage Act, 18 United States Code, Section 1834 (1996). also requires criminal forfeiture of (1) any proceeds of the crime and property derived from proceeds of the crime and (2) any property used, or intended to be used, in commission of the crime.

The EEA authorizes civil proceedings by the Department of Justice to enjoin violations of the act but does not create a private cause of action. This means that anyone believing they have been victimized must go through the US attorney general in order to obtain an injunction.

The EEA is limited to the United States and has no extraterritorial application unless (1) the offender is a US company or a citizen operating from abroad against a US company or (2) an act in furtherance of the espionage takes place in the United States. Other nations lack such legislation, and some may actively support industrial espionage using both their national intelligence services. The US Office of the National Counterintelligence Executive publishes an annual report, mandated by the US Congress, on foreign economic collection and industrial espionage, which outlines these espionage activities of many foreign nations.

Right of Employees to Use Trade Secrets

A perennial source of lawsuits in the trade secrets arena is the employee who is hired away by a competitor, allegedly taking trade secrets along with him. Companies frequently seek to prevent piracy by requiring employees to sign confidentiality agreements. An agreement not to disclose particular trade secrets learned or developed on the job is generally enforceable. Even without an agreement, an employer can often prevent disclosure under principles of agency law. Sections 395 and 396 of the Restatement (Second) of Agency suggest that it is an actionable breach of duty to disclose to third persons information given confidentially during the course of the agency. However, every person is held to have a right to earn a living. If the rule were strictly applied, a highly skilled person who went to another company might be barred from using his knowledge and skills. The courts do not prohibit people from using elsewhere the general knowledge and skills they developed on the job. Only specific trade secrets are protected.

To get around this difficulty, some companies require their employees to sign agreements not to compete. But unless the agreements are limited in scope and duration to protect a company against only specific misuse of trade secrets, they are unenforceable.

Key Takeaway

Trade secrets, if they can be kept, have indefinite duration and thus greater potential value than patents. Trade secrets can be any formula, pattern, device, process, or compilation of information to be used in a business. Customer information, pricing data, marketing methods, sources of supply, and technical know-how could all be trade secrets. State law has protected trade secrets, and federal law has provided criminal sanctions for theft of trade secrets. With the importance of digitized information, methods of theft now include computer hacking; theft of corporate secrets is a burgeoning global business that often involves cyberattacks.

Exercises

1. Wu Dang, based in Hong Kong, hacks into the Hewlett-Packard database and “steals” plans and specifications for HP’s latest products. The HP server is located in the United States. He sells this information to a Chinese company in Shanghai. Has he violated the US Economic Espionage Act?
2. What are the advantages of keeping a formula as a trade secret rather than getting patent protection?

This page titled [18.3: Trade Secrets](#) is shared under a [CC BY-NC-SA](#) license and was authored, remixed, and/or curated by [Anonymous](#).

- **30.3: Trade Secrets** by Anonymous is licensed [CC BY-NC-SA 3.0](#). Original source: <https://courses.lumenlearning.com/waymakerintromarketingxmasterfall2016>.