Trade secrets and software *

Trade secret law provides probably the best protection for the source code of a computer program. It simply requires that you take reasonable efforts to kept the source code secret, such as having agreements to keep it secret from everybody who has access to the source code. There are no formalities, such as filing with a government agency, required.

The Uniform Trade Secrets Act

Misappropriation of trade secrets was initially recognized by the courts as a common-law tort (civil, not criminal, wrong). Recently, most states have adopted the Uniform Trade Secrets Act, making it statutory law. This has given some uniformity to trade secret protection in the United States, and therefore made it easier to be sure you are properly protection your trade secrets.

First, we need to define what a trade secret is. The definition in the Uniform Trade Secrets Act is based on the generally-accepted common law meaning:

> "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
>
> (a) 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
>
> (b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[1]

Note that there are two separate requirements that must be met for a trade secret: it must have economic value because it is not generally known, and it must be protected as a secret. Source code is probably the thing that first comes to mind when you consider things with independent economic value related to computer software. Even though the executable code for a computer program has been widely distributed, the source code cannot be easily reconstructed from that executable code – comments are lost, labels that help one understand data and program structure are gone, as is the history of changes leading to the present version.

But there are other important software development trade secrets, including programmer notebooks that not only detail how something was done, but may explain other techniques that were tried and rejected for one reason or another. Economic value can include not having to go down a dead-end road. In fact, it may be one of the most important trade secret, because it generally cannot be derived from a released program through reverse engineering.

Other important trade secrets are not particular to software development. They include customer lists and pricing information. Microsoft, for example, negotiates pricing with its major customers and requires those customers to keep their prices confidential. The most commonly used example of a trade secret is the formula for Coca Cola.

---

[1] Uniform Trade Secrets Act, §1(4)

It is important that the trade secret not only be something with independent economic value, but also that it can't be readily discovered or recreated by other people. If a technique is learned through legitimate reverse engineering, then its trade secret status is lost. But the definition says "proper means," not "any legal means," so there are some activities that are strictly legal that may be found by a court to be improper.

In one extreme case,[2] the Fifth Circuit affirmed the district court's decision that the photographing from an airplane of a chemical plant under construction was an improper means of discovering the trade secrets embodied in the plant. The court stated its understanding of Texas trade secret law:

> One may use his competitor's secret process if he discovers the process by reverse engineering applied to the finished product; one may use a competitor's process if he discovers it by his own independent research; but one may not avoid these labors by taking the process from the discoverer without his permission at a time when he is taking reasonable precautions to maintain its secrecy. To obtain knowledge of a process without spending the time and money to discover it independently is improper unless the holder voluntarily discloses it or fails to take reasonable precautions to ensure its secrecy.[3]

The second requirement for a trade secret is that it be kept secret. The methods used to protect the secret must be reasonable in light of the nature of what is being kept secret. For example, it may be sufficient to require every salesman for a company having access to the customer list sign an agreement not to disclose it outside of the company. But for a trade secret valued at billions of dollars, such as the formula for Coca Cola, special precautions may be necessary to show that one is diligently protecting the secret.

For software source code, or similar things such as programs supplied as part of a beta test, an agreement not to disclose the material to others without permission will likely suffice as adequate protection. That nondisclosure agreement could be part of a license for the source code or beta test programs, further spelling out how they can and can't be used. Of course, if it appears that the agreement doesn't really matter, or isn't being enforced when a violation is suspected, then it may be found to inadequately protect the trade secret and the trade secret could be lost.

The Uniform Trade Secret Act spells out two ways that a trade secret can be misappropriated. The first is:

> 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.[4]

This means that you somehow found out the trade secret by improper means, rather than by recreating it through reverse engineering or separate development.

> "Improper means" includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means.

---

[2] *E.I. duPont de Nemours v. Christopher*, 431 F.2d 1012, 166 USPQ 421 (5th Cir. 1970).
[3] 431 F.2d at 1015-1016, 166 USPQ at 424.
[4] Uniform Trade Secrets Act, §1(2)(a)(i).

That list is not exhaustive – the court will look to the way one acted to acquire the trade secret. But in many cases it will be clear, such as when a former employee has held onto company documents containing trade secrets and then has used them at his new company.

The second form of misappropriation is when the trade secret is disclosed or used without permission, in contrast to acquiring the trade secret improperly. In particular, it is a misappropriation when there is:

> disclosure or use of a trade secret of another without express or implied consent by a person who:
>
> (A) used improper means to acquire knowledge of the trade secret; or
>
> (B) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was:
>
> (I) derived from or through a person who had utilized improper means to acquire it;
>
> (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
>
> (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or
>
> (C) before a material change of his position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.[5]

Note that the Uniform Trade Secrets Act does not excuse you if you try to claim that you didn't know that something was a misappropriated trade secret. If the circumstances are such that a reasonable person would know that something was wrong, then it is still a misappropriation. Clause (C) addresses the case where somebody got trade secret material through entirely proper means (such as finding it in the seat pocket on an airplane) but it is clear, or becomes clear, that the material is a trade secret (perhaps because it is stamped TRADE SECRET).

Another example would be receiving a trade secret in a fax, email, or regular mail that had been misdelivered. In that case, if you just consider it your lucky day and use the trade secret, you have misappropriated it even though you haven't done any improper act or got it from somebody who acted improperly. However, if you have taken advantage of the trade secret before you would reasonably know that it is a trade secret, that is not a misappropriation.

In the comments to the Uniform Trade Secrets Act, the drafters indicated what could be proper means for acquiring a trade secret:

> 1. Discovery by independent invention;
>
> 2. Discovery by "reverse engineering," that is, by starting with the known product and working backward to find the method by which it was developed. The acquisition of the known product must, of course, also be by a fair and honest means, such as purchase of the item on the open market for reverse engineering to be lawful;
>
> 3. Discovery under a license from the owner of the trade secret;

---

[5] Uniform Trade Secrets Act, §1(2)(a)(ii).

4. Observation of the item in public use or on public display;

5. Obtaining the trade secret from published literature.[6]

There are a number of remedies for the misappropriation of a trade secret – injunctions to prevent you from using, or even threatening to use, the trade secret; ordering the payment of a reasonable royalty for the use of the trade secret; damages caused by the taking or using of the trade secret, including treble damages (actual damages plus twice that amount in exemplary damages – damages to set an example to deter others) in the case of "willful and malicious misappropriation"; and attorney's fees if a party acts in bad faith.

Criminal sanctions

About half the states, including Utah, also have criminal penalties for the misappropriation of a trade secret. Utah's law against theft states:

> 76-6-404. Theft - Elements. A person commits theft if he obtains or exercises unauthorized control over the property of another with a purpose to deprive him thereof.

In the definitions that govern that very general law, trade secrets are explicitly included with other types of property that can be stolen.

> "Property" means anything of value, including ... trade secrets, meaning the whole or any portion of any scientific or technical information, design, process, procedure, formula or invention which the owner thereof intends to be available only to persons selected by him.

And you don't have to take the original trade secret.

> "Obtain" means, in relation to property, to bring about a transfer of possession or of some other legally recognized interest in property, whether to the obtainer or another; in relation to labor or services, to secure performance thereof; and in relation to a trade secret, to make any facsimile, replica, photograph, or other reproduction.

And finally, just because a trade secret owner still has the trade secret after you have taken it doesn't mean that you haven't deprived him of it if you have acted such that its economic value is lost.

> "Purpose to deprive" means to have the conscious object:
>
> (a) To withhold property permanently or for so extended a period or to use under such circumstances that a substantial portion of its economic value, or of the use and benefit thereof, would be lost; ...

Of course, like any other criminal statute, prosecution of those who may have violated the statute can only be brought by a government prosecutor. Since the prosecutor often has crimes considered more important that the theft of a trade secret by a business competitor, it is rare that trade secret misappropriation is treated as theft, even in those states that cover it in their criminal laws.

---

[6] Comments to §1 of the Uniform Trade Secrets Act.

The Economic Espionage Act of 1996

Traditionally, trade secret protection came from state law. But in 1996, Congress got into the act by passing the Economic Espionage Act of 1996. ("Economic espionage" sounds so much more interesting than "trade secret misappropriation.")

> The term economic or industrial espionage is appropriate in these circumstances. Espionage is typically an organized effort by one country's government to obtain the vital national security secrets of another country. Typically, espionage has focused on military secrets. But as the cold war has drawn to a close, this classic form of espionage has evolved. Economic superiority is increasingly as important as military superiority. And the espionage industry is being retooled with this in mind.
>
> It is important, however, to remember that the nature and purpose of industrial espionage are sharply different from those of classic political or military espionage. The phrase industrial espionage includes a variety of behavior – from the foreign government that uses its classic espionage apparatus to spy on a company, to the two American companies that are attempting to uncover each other's bid proposals, or to the disgruntled former employee who walks out of his former company with a computer diskette full of engineering schematics. All of these forms of industrial espionage are problems. Each will be punished under this bill.[7]

Trade secrets are defined essentially the same as in state law:

> "Trade secret" means 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.[8]

The first prohibited activity has to do with actions taken by or for foreign governments.

> Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, 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,

[7] H.R. Rep. 104-788 at 5.
[8] 18 U.S.C. §1839.

replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;

(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in any of paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.[9]

Organizations can be fined not more than $10 million. This provision applies only to foreign governments and two related entities:

The term `foreign instrumentality' means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government.

The term `foreign agent' means any officer, employee, proxy, servant, delegate, or representative of a foreign government.[10]

The second prohibition is a more conventional trade secret law:

Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly –

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.[11]

---

[9] 18 U.S.C. §. 1831.

[10] 18 U.S.C. §1839.

If the offense is committed by an organization, rather than an individual, that organization can be fined not more that $5 million.

Why did Congress feel that there needed to be a federal trade secret law, after over two hundred years of leaving it up to the states? It recognized that while there were existing federal laws that could apply in particular circumstances, there was no general federal trade secret law.

> State laws also do not fill the gaps left by federal law. While the majority of States have some form of civil remedy for the theft of proprietary economic information, either by recognizing a tort for the misappropriation of the information or by enforcing contracts governing the use of the information, these civil remedies often are insufficient. Many companies choose to forego civil litigation because of the difficulties in enforcing a monetary judgment against some defendants which may have few assets or foreign governments with few assets in the United States or because companies do not have the resources or time to bring the civil action. Additionally, private individuals and companies lack the investigative resources necessary to prove that a defendant has in fact misappropriated the proprietary economic information in question. Only a few States have any form of criminal law dealing with the theft of this type of information and most of those laws are misdemeanors, rarely used by State prosecutors.[12]

Congress understated the scope of state trade secret laws. Virtually every state has some form of trade secret law, and 43 states and the District of Columbia have adopted the Uniform Trade Secret Act. And about half the states, not "only a few," have criminal provisions addressing trade secrets.

Perhaps the concerned businesses should have been convincing the states that don't have criminal penalties for trade secret theft to pass such laws. But it's always easier to convince only one legislative body – Congress – rather than fifty, and there is some argument for uniformity across the country. Also, by passing the Economic Espionage Act, both Congress and federal law enforcement agencies like the Department of Justice and the Federal Bureau of Investigation get to be involved in trade secret protection.

In keeping with the argument that this legislation was enacted to address the stealing of industrial secrets by foreign governments and agents, Congress extended the reach of the law outside the borders of the United States.

> This chapter also applies to conduct occurring outside the United States if –
>
> (1) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or
>
> (2) an act in furtherance of the offense was committed in the United States.[13]

---

[11] 18 U.S.C. § 1832.

[12] H.R. Rep. 104-788 at 6-7

[13] 18 U.S.C. § 1837.

Because the thought of Federal criminal law protecting trade secrets, and especially stiff penalties for violations, caused concern, the sponsors tried to indicate that the legislation wasn't as sweeping as it seems.

> This legislation is not intended to apply to innocent innovators or to individuals who seek to capitalize on the personal knowledge, skill, or abilities they may have developed. The statute is not intended to be used to prosecute employees who change employers or start their own companies using general knowledge and skills developed while employed. It is the intent of Congress, however, to make criminal the act of employees who leave their employment and use their knowledge about specific products or processes in order to duplicate them or develop similar goods for themselves or a new employer in order to compete with their prior employer.
>
> H.R. 3723 has been drafted so as to minimize the risk that the statute will be used to prosecute persons who use generic business knowledge to compete with former employers. For example, under the new offense the government is required to prove that the defendant has wrongfully copied or otherwise exerted control over a "trade secret." The definition of trade secret requires that the owner of the information must have taken objectively reasonable and active measures to protect the information from becoming known to unauthorized persons. If the owner fails to attempt to safeguard his or her proprietary information, no one can be rightfully accused of misappropriating it. It is important to note, however, that an owner of this type of information need only take "reasonable" measures to protect this information. While it will be up to the court in each case to determine whether the owner's efforts to protect the information in question were reasonable under the circumstances, it is not the Committee's intent that the owner be required to have taken every conceivable step to protect the property from misappropriation.[14]

Of course, the line between what is "generic business knowledge" and what is a "trade secret," especially when the information is learned at one's job, is not a clear line. Employers certainly would like their past employees to go into some other line of work, rather than going to work for a competitor, so that the competitor can't benefit from the experience that the employee has gotten with the past employer.

Trade secret litigation

While trade secrets protection is quite easy to get – you have something of commercial value that you keep secret – it can be quite difficult to enforce. The most difficult part of many trade secret misappropriation cases is for the plaintiff to say what the secret is with sufficient precision. That is necessary because simple fairness (and many court decisions) dictate that the defendant needs to know what the secret is to be able to show that it is not really a secret, was obtained lawfully, or isn't being used.

This isn't difficult in the most common type of trade secret protection for digital material – where a former employee or a licensee with access to the source code for a

[14] H.R. Rep. 104-788 at 7.

computer program has used that knowledge to produce a competitive product. Things that a court would consider in that instance are similar to what is considered for copyright infringement: whether the two programs show substantial similarity in the absence of some other reason besides misappropriation. In fact, many times the complaint of trade secret misappropriation is combined with a charge of copyright infringement in a single case. (The case will then end up in federal court, even though trade secret misappropriation is a state claim, as an adjunct to the federal copyright claim.) The court may also consider how rapidly the defendant's program was developed as an indication of misappropriation.

But when the trade secret is something less precise than the source code for a program, such as a technique for doing something, things become more complicated. It is necessary to say what the technique is and how and when it was acquired from the plaintiff by the defendant.

In many instances, the court will require that the plaintiff specify the particular trade secrets before he is allowed to review the source code for the defendant's program, to prevent the plaintiff from mining the defendant's program for similarities and then claiming that they are misappropriated trade secrets. But this requires the plaintiff to make a guess about how the defendant's program is written and what trade secrets it may contain.

Care has to be taken so that each parties' trade secrets are not revealed to the other party or the public during the litigation. This often requires that each side hire an independent expert to examine the material from the other side, under a protective order from the court limiting what can be disclosed.

To make enforcement of trade secrets less uncertain, there are a number of things that can be done. First, identify any trade secrets before or at the time they are being told to somebody. This could be as simple as saying that all the source code about to be shown is a trade secret, or as complex as having to identify what parts of the documentation or discussion of a technique or business method are trade secrets and what parts are generally known. There should be a signed agreement, indicating the nature of any trade secrets in place before they are disclosed. And anybody receiving a trade secret should be reminded every once in a while that the material is considered a trade secret and should not be disclosed to another or used in any way without permission.