

**PROTECTION OF TRADE SECRETS A COMPARISON:
THE ECONOMIC ESPIONAGE ACT OF 1996 AND
THE UNIFORM TRADE SECRETS ACT
by Kevin J. Collette
Update Bulletin**

One of your employees left with what you consider to be a vital trade secret. That information is now in the hands of your competitor and the employee is now employed by them. You search your company's documents and find you have no employment, nondisclosure or noncompetition agreement with the ex-employee and no written policies protecting your information. What legal remedies do you have then to protect your trade secrets?

State Law. Trade secrets are generally governed by state law and most states have adopted the Uniform Trade Secrets Act (the "UTSA"). The UTSA was adopted with only a minor change by the Washington legislature in 1981 and it is codified in RCW 19.108.

Federal Law. In 1996, the U.S. Congress passed The Economic Espionage Act (18 U.S.C. §§ 1831-1839) (the "Act") to extend federal protection of intellectual property to trade secrets.

Remedies. One may pursue civil actions under state law for theft of trade secrets. The Act subjects those accused of theft to possible federal criminal investigation, prosecution, and potentially severe punishment. Also, in Washington and a growing number of states, theft of a trade secret is also a crime. See, e.g. RCW 9A.56.020 defining theft and RCW 9A.56.010(5) specifying trade secrets.

A. Definitions of Trade Secrets.

1. Act. The Act defines a trade secret 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 public¹ (18 U.S.C. § 1839(3))."

2. The Uniform Trade Secrets Act (UTSA). The UTSA defines a trade secret as:

"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 (U.T.S.A. § 1)²."

3. Differences in Definitions.

The definition in the Act is much more detailed to protect not only existing and emerging technologies in companies but also those generally in the U.S. In addition, while the UTSA requires the information to be of value to others, the Act merely requires the information to be of value to the owner.

B. Definitions of Theft.

The Act defines the theft of trade secrets as follows:

"(a) 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 be punished as provided by this statute³ (180 US.C. § 1832)."

The Act describes the transgression as "theft" while the UTSA labels it "misappropriation." This is because the former is a criminal law while the latter is civil. Nonetheless the basic definition is remarkably similar. Under the UTSA, misappropriation means:

- (a) 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; or
- (b) disclosure or use of a trade secret of another without express or implied consent by a person who:
 - (i) used improper means to acquire knowledge of the trade secret; or

- (ii) at the time of disclosure or use, knew or had reason to know that his or her knowledge of the trade secret was (A) derived from or through a person who had utilized improper means to acquire it, (B) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use, or (C) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use.
- (iii) before a material change of his or her 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 (U.T.S.A. § 1).⁴

The Act is much more complete in dealing with stealing, unauthorized copying, and impermissible receiving than the UTSA, again to cover all types of new and future technologies. The Act definition also differs from the UTSA definition in three important ways:

- 1) It is a crime to deprive the rightful owner of trade secrets in some way if it creates an economic benefit for the thief or a third party. This economic benefit requirement can be satisfied simply by depriving the rightful owner of the information.
- 2) A third party who acquires a trade secret from someone else is guilty of theft only if they know that the trade secret was misappropriated, while the UTSA holds the third party liable if they knew or had reason to know the information was purloined; and
- 3) The Act extends the scope of criminal liability by criminalizing attempts and conspiracies to steal trade secrets.⁵

Proving Theft or Misappropriation.

The Act provides a clear definition of theft, but there is no way to know how easy or difficult it will be to prove. Because of the similarities with the UTSA definitions, however, the UTSA can shed some light on the process. There are three elements to a claim for misappropriation under the UTSA: (1) secrecy; (2) novelty, and (3) economic value.

1. Secrecy

If the information is not maintained in secret, it will not be entitled to protection by the courts. Failure to take internal and external security measures such as making documents "proprietary" or "confidential" informing employees/contractors that particular matters are secret, limiting access to information on a "need-to-know" basis, having employees/contractors sign confidentiality agreements, and conducting comprehensive exit interviews, may negate the existence of a trade secret.

2. Novelty

If others generally know or can readily learn the information, then it will not meet the novelty requirement. The information cannot be common knowledge within an industry.

3. Economic Value

If the information is not valuable to the owner or would not be valuable to a competitor, then it will not meet the economic value requirement. This may include information with potential, rather than actual, value, such as a product or process still in the development stage.

Those trade secrets meeting the above tests may be protected against misappropriation. Then, the plaintiff must prove that the defendant actually took the information.⁶ Because there is so much shared information today, it can be quite difficult to show that the defendant did not independently develop the same process or technique that is the subject of the trade secret. Often the most convincing proof is that the defendant had access to the trade secrets at one time⁷ or is caught in the act of stealing. It is quite difficult, therefore, to prove misappropriation under the UTSA.

Congress was cognizant of this problem in enacting the Act. It remains to be seen, however, whether it will be easier to prove theft under the Act than to prove misappropriation under the UTSA. Because it is a federal criminal law the Justice Department will conduct criminal investigations, which might prove more effective than civil discovery. On the other hand, since the Act is a criminal statute, theft must be proven beyond a reasonable doubt which is a much higher burden than exists under civil statutes.

It is also difficult to predict the willingness of the Justice Department in pursuing cases of trade secret theft. There are a few other laws that criminalize the misuse of intellectual property, which may indicate how the Act might be applied. There is a provision of the Copyright Act that makes it a crime to willfully infringe a copyright⁸, and a federal criminal law against the purposeful deceptive misuse of trademarks.⁹ The Justice Department has used these statutes to prosecute a number and variety of cases. Counterfeit trademark cases have ranged from an elaborate operation selling mislabeled hair care products¹⁰ to the sale of counterfeit watches at a swap meet.¹¹ Copyright cases have similarly run the gamut from the serious to the picayune. Some have dealt with very small-time copying, including one case dealing with a single video store's copying a few dozen videos for rental.¹² The Justice Department appears to prosecute high profile cases and cases where the aggrieved party actively complains and forces an investigation. In all likelihood they will use a similar approach in dealing with trade secret cases.

Punishment

Individuals convicted of stealing trade secrets will be "fined under this title or imprisoned not more than 10 years."¹³ Any organization found guilty "shall be fined not more than \$5,000,000."

The Act includes other punishments that could prove potentially devastating, particularly forfeiture provisions.

The court, in imposing sentence on a person for a violation of this chapter, shall order, in addition to any other sentence imposed, that the person forfeit to the United States -

- (1) any property constitution, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and
- (2) any of the person's property used, or intended to be used, in any manner or part, to commit or facilitate the commission of such violation, if the court in its discretion so determines, taking into consideration the nature, scope, and proportionality of the use of the property in the offense.¹⁴

The Legislative History says that there will be criminal forfeiture of the proceeds of the crime "and limited forfeiture of the property used to commit the crime."¹⁵ Unfortunately the law itself is not so limiting. And, perhaps more importantly, other similar forfeiture provisions have been aggressively applied.

These criminal punishments add to the existing remedies available under state law. The act specifically states that the Act will not "preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession or territory law for the misappropriation of a trade secret."¹⁶ Therefore, existing remedies are still available, and it is possible to bring a civil action in conjunction with or after the criminal case.

A few states criminalize the theft of trade secrets, but as the legislative history for the Act states, these laws "are rarely used by State prosecutors."¹⁷ In the State of Washington, "theft" is defined in RCW 9A.56.020 as follows:

- (a) To wrongfully obtain or exert unauthorized control over the property or services of another or the value thereof, with intent to deprive him of such property or services; or
- (b) By color or aid of deception to obtain control over the property or services of another or the value thereof, with intent to deprive him of such property or services; or
- (c) To appropriate lost or misdelivered property or services of another, or the value thereof, with intent to deprive him of such property or services.

Further, the term "deprive" is defined in RCW 9A.56.010(5) to mean as follows:

"Deprive" in addition to its common meaning means to make unauthorized use or an unauthorized copy of records, information, data, trade secrets, or computer programs."

It is much more common for businesses who feel that they have been the victim of theft to bring a civil action under the applicable state law, which is most commonly a version of the UTSA.

The most common remedies for "actual or threatened misappropriation are injunctions and damages."¹⁸ The injunction can be of limited duration, or in some situations can run as long as the information remains a valuable trade secret.¹⁹ The plaintiff may also recover damages for actual loss, and unjust enrichment if not included in actual damages.²⁰ In cases of willful or malicious misappropriation, the court may award exemplary damages "in an amount not exceeding twice" the actual damages." Attorney fees may also be awarded in cases of willful or malicious misappropriation, as well as when a claim is brought in bad faith, or a motion to terminate an injunction is made or resisted in bad faith.²¹ Finally, in some rare cases the court may determine that the defendant would be unfairly burdened if prohibited from using the trade secret, and so "an injunction may condition future use upon payment of a reasonable royalty" for the duration of the usefulness of the trade secret.²²

Conclusion

The Act provides for federal criminal protection for trade secrets. Actions that were a civil statutory violation under the UTSA may now be a federal criminal offense, and actions that are currently actionable in civil litigation with awards of damages and injunctions are now punishable by fines, imprisonment and forfeiture of property under the Act. Otherwise, the Act does not bring major changes to either the definitions of trade secrets or of theft.

We will have to wait to see if the Justice Department will actively pursue cases and how quickly they are resolved.