BioProcess™ INTERNATIONAL

A Brief History of Trade Secret Law, Part 2

by Ernie Linek

Reprinted with permission from BioProcess International 2(10):20-26 (November 2004)

Everyone has heard of trade secrets. Employees are often asked to sign an agreement regarding their protection, whereas employers often worry that employees will move to a competitor and take the company's trade secrets with them. The Internet appears to contain information on every company now in business (and many no longer in business). Much of the public corporate information now available online would have been viewed as trade secret information just a few years ago.

What is a trade secret today? Are trade secrets still important? Are there any left to protect? If yes, how can those secrets be protected in today's information age? Part one of this article (in *BioProcess International*'s October issue) discussed legal definitions of trade secrets in the United States and their implications for protection. Part two discusses federal enforcement provisions and specific methods companies can use to protect their trade secrets.

The Economic Espionage Act of 1996 (EEA)

Although the Uniform Trade Secrets Act (UTSA) was a valuable update of the laws designed to protect trade secrets, clearly more was needed, particularly on a federal level, because the states did not uniformly adopt the act.

In 1996, Congress passed the EEA to close a federal enforcement gap in this important area of intellectual property law and in recognition of the increasing importance of the value of intellectual property in general (and trade secrets in particular) to the economic well-being and security of the United States. The EEA's definition of trade secrets is even broader than those of the UTSA (1) and the 1939 Restatement of Torts (2). It defines trade secrets 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. (3)

Illustration by C.A. Scott using photographs from Photos.com

In addition to the broad definition of trade secrets, the EEA includes both civil and criminal penalties for violations. It is not intended to criminalize every theft of trade secrets for which civil remedies may exist under state laws (such as under the UTSA). Appropriate discretionary factors that the US Justice Department

will consider in deciding whether to initiate a criminal prosecution under the EEA include the scope of criminal activity (including evidence of involvement by a foreign government, foreign agent, or foreign instrumentality); the degree of economic injury to the trade secret owner; the type of trade secret misappropriated; the effectiveness of available civil remedies; and the potential deterrent value of prosecution.

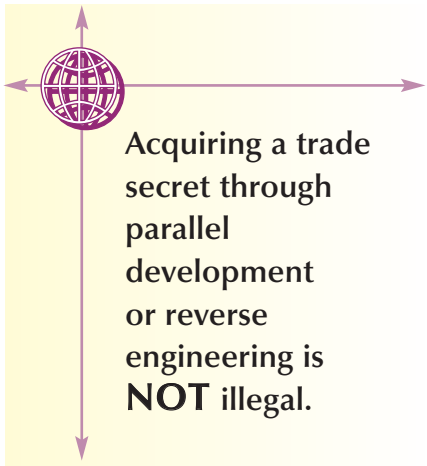
Some acts prohibited by the EEA include unauthorized taking, copying, and receiving of trade secrets. The EEA also prohibits any attempt at such activity or conspiracies with others to engage in such activity. Moreover, the statute broadens this description to include any possible means of committing the offending acts, including all forms of electronic activity. The EEA covers not only the activities of corporations, but also those by and on behalf of foreign governments.

Foreign Activity (Economic Espionage): The EEA prescribes a fine of up to $500,000 or imprisonment for not more than 15 years (or both) to anyone who commits the prohibited acts intending or knowing that such events will benefit a foreign government, instrumentality, or agent.

Domestic Activity (Theft of Trade Secrets): The EEA similarly prohibits taking, copying, or receiving trade secrets without authorization in the domestic context for those trade secrets that are related to or included in a product and placed in interstate or foreign commerce.

The statute adds three requirements that are not present with regard to espionage on behalf of foreign governments or instrumentalities. The wrongful conduct must

- be committed with the intent to convert the trade secret
- economically benefit anyone other than the owner, and
- be committed with the intent or knowledge that the offense will injure the owner of the trade secret.



A domestic offense also carries criminal penalties of up to 10 years, making the penalties for US violations somewhat less severe than those related to foreign activity. For foreign activity, the EEA protects against the conveyance of merely a "benefit," rather than an "economic benefit," as for domestic activity. This recognizes that the benefit bestowed on a foreign government or instrumentality need not be an economic one.

Violators of the EEA are subject not only to the criminal penalties described above, but to the forfeiture of any proceeds obtained by the violator, either directly or indirectly, as a result of such violation. Moreover, the violator's property used or intended to be used to commit or facilitate the commission of the violation can be seized by the US government.

The US Justice Department may also use a civil action to seek and maintain appropriate injunctive relief against violation of the EEA. The EEA provides no injunctive relief to private parties. They must continue to resort to the traditional civil injunctive remedies of state courts.

The EEA clearly has a global reach by extending beyond the borders of the United States when an offender is a citizen or permanent resident alien of the United States or is an organization organized under the laws of the United States or a state or political subdivision thereof. The EEA also applies to conduct outside the United States if an act to further such conduct was committed inside the United States.

The EEA does not expressly provide for any defenses. However, the legislative history of the EEA suggests that defenses traditionally available in a civil action for theft of trade secrets are equally applicable to defend against criminal charges. Specifically, the legislative history indicates that acquiring a trade secret through parallel development or reverse engineering is not illegal.

Parallel Development: The owner of a trade secret, unlike the holder of a patent, does not have an absolute monopoly on the information or data that compose it. Other companies and individuals have the right to discover the elements of a trade secret through their own research and hard work. In 1974, the Supreme Court recognized this fact, stating:

> If something is to be discovered at all, very likely it will be discovered by more than one person. . . . Even were an inventor to keep his discovery completely to himself, something that neither the patent nor trade secret laws forbid, there is a high probability that it will be soon independently developed. If the invention, though still a trade secret, is put into public use, the competition is alerted to the existence of the inventor's solution to the problem and may be encouraged to make an extra effort to independently find the solution thus known to be possible. (**4**)

Reverse Engineering: Similarly, a person can legally discover the elements of a trade secret by *reverse engineering*, the practice of taking something apart to determine how it was made or manufactured. The Supreme Court recognized this important fact as well, stating that the law does not protect the owner of a trade secret from "discovery by fair and honest means, such as independent invention, accidental disclosure, or by so-called reverse engineering" (**4**).

The EEA does not expressly address when reverse engineering would be a valid defense; however, legislative history suggests that "the

The proper focus of inquiry is not whether an alleged trade secret can be deduced by reverse engineering, but whether IMPROPER means are required to access it.

important thing is to focus on whether the accused has committed one of the prohibited acts of this statute rather than whether he or she has reverse engineered. If someone has lawfully gained access to a trade secret and can replicate it without violating copyright, patent, or this law, then that form of reverse engineering should be fine" (**5**).

Therefore, to avoid a successful claim by a defendant that he discovered the trade secret by reverse engineering, the means by which that defendant misappropriated the trade secret should be established. Furthermore, a defendant cannot defeat a criminal prosecution simply by claiming the trade secret could have been discovered by reverse engineering. The proper focus of inquiry is not whether an alleged trade secret can be deduced by reverse engineering but rather, whether improper means are required to access it.

A Few Reported EEA Cases

June 2002: Two people were arrested in California on a federal complaint issued out of federal court in Boston charging them with theft of trade secrets from Harvard Medical School's Department of Cell Biology while they were research fellows. They were charged in a criminal complaint with conspiracy, theft of trade secrets, and interstate transportation of stolen property. The charges arose out of the alleged theft of certain trade secrets belonging to Harvard Medical School, including reagents made and used by the school to develop new immunosuppressive drugs for controlling organ rejection and also to study the genes that regulate an important signaling enzyme in the heart, brain, and immune systems.

It is alleged that the individuals each signed a participation agreement upon coming to Harvard, in which they agreed that all rights to any invention or discovery conceived or first reduced to practice as part of, or related to, their university activities were assigned to Harvard, and that their obligations would continue after termination of their Harvard employment. It is alleged that despite their legal and contractual obligations, they took and conspired to take proprietary and highly marketable scientific information belonging to Harvard with the intention of profiting from it by collaborating with a Japanese company to create and sell related and derivative products or otherwise capitalize on the information.

If convicted, they each face a maximum sentence of five years' imprisonment on the conspiracy charge, 10 years on the theft of trade secrets charge, and 10 years on the interstate transportation of stolen property charge. Additionally, the defendants face a maximum fine of $250,000 on each of the charges, and any prison term would be followed by three-years of supervised release.

May 2002: In another case, the US Attorney for the Northern District of Ohio announced that an accused pled guilty to a one-count *Information* (a formal criminal charge filed by a prosecuting attorney without the aid of a grand jury), charging him with making false statements to the government. The Information charges that on 2 September 1999, the accused provided a materially false, fictitious, and fraudulent statement in an interview with special agents of the Federal Bureau of Investigation, who were investigating the theft of research and materials from the Cleveland Clinic Foundation (CCF). The accused falsely understated the number of vials of research material that had been taken from a laboratory by a second defendant, by initially indicating that 10 or fewer vials had been taken, when in fact, several hundred vials were taken.

An indictment is still pending against the second defendant, charging him with conspiracy, economic espionage act offenses, and transporting stolen property in interstate and foreign commerce. Defendant 2 is alleged to have conspired to steal from the CCF DNA and cell line reagents and constructs developed by researchers at CCF and to have committed two counts of economic espionage by stealing trade secrets and altering and destroying them.

In 2004, the Tokyo High Court turned down a request to extradite Defendant 2 to the United States to stand trial on industrial espionage charges, marking Japan's first rejection of an extradition request from American authorities.

January 2002: The US Attorney announced that two defendants were sentenced after entering guilty pleas to a two-count indictment charging them with conspiracy to convey trade secrets and the substantive offense of conveying trade secrets.

Defendant 1 was sentenced to 14 months confinement (seven to be served in a community correctional center), two years supervised release, and a special assessment of $200. Defendant 2 was sentenced to 10 months confinement (five in a community correctional center), two years supervised release, and a special assessment of $200.

These defendants were convicted of conspiring to convey trade secrets and conveying trade secrets. Defendant 1 obtained numerous pieces of proprietary information owned by RP Scherer, Inc. (RPS) from a friend in Florida. The information included gel formulas, fill formulas, shell weights, and experimental production order

(EPO) data. This information was known by the defendant to be proprietary information and trade secrets of RPS. Defendant 1 and Defendant 2 attempted to sell the information to NPB, a competitor of RPS.

NPB actively cooperated with federal authorities and the victim corporation. Without the assistance of this competitor corporation, the successful prosecution of this case would not have been possible.

Take-Home Lessons

What does all of this mean to a reader of this publication — as an employee or an employer?

Trade Secrets Still Exist, and They Are Protectable Under Both Federal and State Law: Employers and employees must make adequate efforts to protect secrets for them to remain valid. For example, when a new discovery is made you have three choices:

- Announce your discovery to the world — make it public. You receive instant recognition for the discovery but no right to prevent others from copying it.
- Patent the discovery so you can have the right to exclude others from using it for up to 20 years — if a patent issues.
- Keep the discovery a secret. It is your property and it gives you a competitive advantage. Why disclose it to others? Patents, if granted, don't last forever, so keep it secret — unless the secret is easy to reverse engineer or you fear parallel development.

A Trade Secret Can Last Forever — As Long As You Keep It a Secret: Think of the formula for Coca-Cola®. A search of the Internet for the "formula" reveals many, many guesses — each claiming to be the real deal. It is likely that the formula for Coca-Cola® has been modified more than once since the original version was first sold in 1886, but only the owner of the trade secret — The Coca-Cola Company — knows the actual formula.

Keeping a Trade Secret "Secret" Can Be Difficult: Again, the Coca-Cola® formula is a prime example. As a search of the Internet shows, many people have tried and are likely still trying to duplicate the "secret" formula. Some do it to satisfy their intellectual curiosity. Others do it to make a competitive product. If your trade secret can be determined by reverse engineering, you can be sure that someone will find it.

In addition to reverse engineering, you can lose your trade secret in other ways. If visitors to your company can learn your secrets, they may do so. Former employees may take your secrets with them. Employment agreements may be needed to reinforce employee recognition of the importance of protecting your trade secrets. And if you enter into a joint development agreement with another company and fail to protect your trade secrets, they may no longer be protectable even before that development agreement ends.

A Sample Employment Agreement

EMPLOYEE AGREEMENT REGARDING CONFIDENTIAL INFORMATION

I, the undersigned employee, in consideration of my employment or continued employment in any capacity with _____ [hereafter, THE COMPANY], the salary or wages paid for my services in the course of such employment, and the use of the facilities and experience of THE COMPANY, and of the opportunity given by THE COMPANY to me to acquire CONFIDENTIAL INFORMATION or PROPRIETARY INFORMATION relating to the business of THE COMPANY, voluntarily agree as follows:

I agree to keep secret and not to disclose any CONFIDENTIAL INFORMATION or PROPRIETARY INFORMATION of THE COMPANY, including information received in confidence by THE COMPANY from others, either during or after my employment with THE COMPANY, except upon written consent of THE COMPANY.

I understand that the terms CONFIDENTIAL INFORMATION and PROPRIETARY INFORMATION are used by THE COMPANY to identify valuable and protectable business information which may be used in conducting the business of THE COMPANY and which may give THE COMPANY an opportunity to obtain an economic advantage over competitors who do not know it or use it. This includes information that I conceive or develop as well as information that I learn from other employees of THE COMPANY.

I will not, except as THE COMPANY may otherwise consent or direct in writing, reveal, or disclose, sell, use, lecture upon, or publish any CONFIDENTIAL INFORMATION or PROPRIETARY INFORMATION of THE COMPANY, or authorize anyone else to do these things at any time either during or subsequent to my employment with THE COMPANY.

I understand that this Agreement shall continue in full force and effect after termination of my employment. Provided however, that my obligations under this Agreement shall cease when any specific CONFIDENTIAL INFORMATION or PROPRIETARY INFORMATION of THE COMPANY becomes publicly known through the activities of another, without my direct or indirect aid or assistance.

EMPLOYEE's NAME: _____ EFFECTIVE DATE: _____

EMPLOYEE's SIGNATURE: _____ WITNESS: _____

Can I Use Both Patent Law and Trade Secret Law to Protect the Same Discovery? Generally — no. The patent laws of the United States require full disclosure of an invention, including the best mode (the base way to make and use the invention) known or contemplated by its inventor when the patent application is filed. Any attempt to keep part of the invention a trade secret would invalidate the patent because the "best mode" would not be disclosed. On the other hand, improvements of an invention, made after filing a patent application, could be preserved as trade secrets — but not if another patent application were to be filed.

What Are Some Advantages to Maintaining a Trade Secret? A trade secret can give you an edge over the competition in manufacturing, particularly if the secret cannot easily be reverse engineered. A trade secret can be used by a seller to bind a prospective purchaser or subcontractor to secrecy regarding how a product is made.

What Are Disadvantages to Maintaining a Trade Secret? Reverse engineering, parallel development, and inadvertent disclosures — anyone who has lawfully acquired a trade secret may use it without liability unless he acquired it subject to a contractual limitation or restriction regarding its use. For many products, trade secret protection is therefore not feasible because the nature of the product can be readily determined by any purchaser, either directly by inspection or by reverse engineering.

When Should We Choose Trade Secret Protection Instead of Patent Protection? Trade secret protection should be relied upon if an invention is not patentable. Furthermore, trade secret protection also may be relied on when the process or product is one that can be readily maintained as a secret because it defies reverse engineering (such as the Coca-Cola® formula) so that the period of exclusivity can extend beyond the 20-year maximum term of a patent.

What Are Some Disadvantages of Trade Secret Protection Compared with Patent Protection? During the lifetime of a US utility patent (up to 20 years from the filing date), the patentee has the right to seek injunctive relief and monetary damages from a federal court based on the unauthorized making, using, selling, or offering for sale of the invention claimed in the patent. There is no defense in patent law based on parallel development or reverse engineering.

The owner of a trade secret, depending on the law of his state (or the decision of the Department of Justice), may (or may not) have similar rights to seek an injunction or monetary damages — provided that there is a defined and protectable trade secret that has been misappropriated by the accused. Under some state laws (and the common law) the trade secret owner has almost no rights except against those who have contracted, expressly or by implication, not to disclose the secret or who have obtained it unfairly. Further, if a trade secret is disclosed to the public by a breach of confidence, the secret dissolves, and the former trade secret holder generally has no recourse against new users.

What Steps Can a Company Take to Discourage Subcontractors from Giving Its Trade Secrets to Other Companies? In addition to using confidentiality agreements between you and any outsider that does work for you, your company should stamp a notice, such as the following, on each document sent out (check with your local attorney for specific requirements of your state):

> **Notice to All Persons Receiving This Document**
> This document contains proprietary information and is the property of ABC, Inc. ("ABC") and is delivered to you on the express condition that it is not to be disclosed, reproduced in whole or in part, or used for manufacture for anyone other than ABC without ABC's prior written consent; and that no right is granted to disclose or use any information contained in this document, other than as authorized by ABC.

What Steps Can a Company Take to Discourage Its Employees from Taking or Giving Its Trade Secrets to New Employers or Other Companies? Employment agreements can be useful as an effort to protect your trade secrets. Check with your local attorney for specific requirements of your state. A sample agreement on this subject is shown in the box accompanying this article.

References

1 *The Uniform Trade Secrets Act* ("UTSA") is model legislation drafted by the National Conference of Commissioners on Uniform State Laws. A hard copy with commissioners' comments on the various sections can be ordered from the National Conference of Commissioners on Uniform State Laws, 676 North St. Clair Street, Suite 1700 Chicago, Il 60611.

2 *Restatement of Torts,* Section 757, Comment b (1939).

3 Economic Espionage. *US Code,* Section 1831 et seq., Title 18, 1996: www4.law.cornell.edu/uscode/18/1831.html.

4 Kewanee Oil Co. v. Bicron Corp., 416 US 470: 490–491 (1974).

5 142 *Congressional Record*, S12201, S12212 (daily edition, 2 October 1996).

Ernie Linek *is senior partner at Banner & Witcoff, Ltd., 28 State Street, 28th Floor, Boston, MA 02109-1775, ELinek@bannerwitcoff.com.*