FENWICK & WEST LLP

Trade Secrets Protection

A Primer and Desk Reference for Managers and In House Counsel

FENWICK & WEST LLP

About the Firm

Fenwick & West LLP provides comprehensive legal services to high technology and biotechnology clients of national and international prominence. We have over 250 attorneys and a network of correspondent firms in major cities throughout the world. We have offices in Mountain View and San Francisco, California.

Fenwick & West LLP is committed to providing excellent, cost-effective and practical legal services and solutions that focus on global high technology industries and issues. We believe that technology will continue to drive our national and global economies, and look forward to partnering with our clients to create the products and services that will help build great companies. We differentiate ourselves by having greater depth in our understanding of our clients' technologies, industry environment and business needs than is typically expected of lawyers.

Fenwick & West is a full service law firm with nationally ranked practice groups covering:

- Corporate (emerging growth, financings, securities, mergers & acquisitions)
- Intellectual Property (patent, copyright, licensing, trademark)
- Litigation (commercial, IP litigation and alternative dispute-resolution)
- Tax (domestic, international tax planning and litigation)

Intellectual Property Group

Fenwick & West's Intellectual Property Group offers comprehensive, integrated advice regarding all aspects of the protection and exploitation of intellectual property. From providing sophisticated legal defense in precedent-setting user interface copyright lawsuits to prosecuting arcane software patents, and from crafting user distribution arrangements on behalf of high technology companies to implementing penetrating intellectual property audits, our attorney's technical skills enable the Firm to render sophisticated legal advice.

Our Offices

Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel: 650.988.8500
Fax: 650.938.5200

Embarcadero Center West
275 Battery Street
San Francisco, CA 94111
Tel: 415.875.2300
Fax: 415.281.1350

For more information about Fenwick & West LLP, please visit our Web site at: www.fenwick.com.

Trade Secrets Protection

A Primer and Desk Reference for Managers and In House Counsel

Table of Contents

Introduction

Companies sometimes overlook trade secrets as intellectual property assets because both their creation and continued existence depend upon secrecy. It is unlikely that a company will issue announcements or press releases that a trade secret has been created. Unlike patents, copyrights or trademarks, trade secrets are not publicly recognized or registered with the government.

Thus, when managers and corporate counsel periodically take stock of their company's intellectual property assets, they may fail to grasp the full extent of the company's trade secrets portfolio. Depending on the industry in which the company competes and the technology on which the company's business is based, this oversight could be a costly mistake. The trade secrets portfolio may in fact be more valuable than all of the company's patents, copyrights and trademarks combined.

Trade secrets are easily misappropriated because they represent nothing more than information, which can be memorized, scribbled down, e-mailed or copied onto some tangible medium and then quietly removed from company premises. Once trade secrets fall into the hands of an unscrupulous competitor or former employee, they can be clandestinely put to immediate use. Depending on the nature of the trade secrets, a competitor or former employee may be able to take and make use of the secrets without getting caught. For example, if the trade secrets involve a timesaving or cost-saving step for a manufacturing process, they could be implemented inside a competitor's facility without the rightful owner's knowledge or suspicion.

The mobility of the workforce in today's knowledge-based economy heightens the risk of misappropriation. Employee turnover is rapid; and employers use consultants and contractors even in highly sensitive jobs. But it is the company's responsibility to protect its trade secrets. Who is keeping track of what trade secrets these workers bring with them from their previous employers and what trade secrets they take when they leave?

To police your company's trade secrets portfolio, the first step is to acquire a working knowledge of trade secret law in order to spot potential issues and problems. In California, as in most other states, a patchwork of state and federal laws (including case law) addresses the protection of trade secrets. The Uniform Trade Secrets Act provides a starting point in this analysis but it is by no means the exclusive source of law. This guide provides a quick reference to the basic laws and legal principles in California law. State trade secrets laws are similar but vary from state to state.

What Is a Trade Secret?

Like the majority of states, California has adopted a version of the Uniform Trade Secrets Act (UTSA). Enacted in 1984, the UTSA is codified under Section 3426 to 3426.11 of the California Civil Code.

Statutory Definition
The version of the UTSA adopted by California defines a "trade secret" as follows:

"Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and

(2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Four Basic Elements
Each of four elements must be present in a "trade secret":

- A "trade secret" must consist of *information*. The types of information that have been protected by trade secret law are virtually without limit. The most common examples fall under two categories: technical information and business information. In the next section, you will see some examples.
- The information must derive *economic value* (actual or potential) from the fact that it is secret. In other words it must have some value flowing from the fact that it is not known, and therefore cannot be put to use, by others. This value is independent of any intrinsic value that the information might have. To look at this element in still another way, information has the requisite independent economic value if a potential competitor or other interested person would have to expend time and money to find or develop it.
- The information *cannot be generally known* (either by the public, or, more importantly, by other persons in the industry). To be a trade secret, the information must not be generally known to the public, industry competitors, or others who could realize economic value from its disclosure or use. Knowledge of the information in question by even a very small number of outsiders (say, one key person) can deny or destroy trade secret status. As the Comments to the UTSA state, "[i]f the principal person who can obtain economic benefit from information is aware of it, there is no trade secret." Keep in mind, however, that unique combinations of generally known concepts *can* be a trade secret.

- The information must be treated as a secret, and be *the subject of reasonable efforts* to maintain its secrecy. For information to acquire and maintain trade secret status, its owner must exercise reasonable efforts to maintain its secrecy. The owner's mere desire or intent to keep information a secret is not enough.

But what efforts are considered "reasonable"? The comments to the UTSA state, "[t]he courts do not require that extreme and unduly expensive procedures be taken to protect trade secrets against flagrant Industrial espionage."

A California federal court has defined "reasonable efforts" to include "advising employees of the existence of a trade secret, limiting access to the information on a 'need to know basis,' requiring employees to sign confidentiality agreements, and keeping secret documents under lock." Requiring employees, contractors, visitors and other people who may come into contact with trade secret information to sign confidentiality or non-disclosure agreements help to ensure that the information retains its trade secret status, because such agreements impose on their signers a contractual duty not to disclose the information.

Examples of Trade Secrets

Trade secrets largely fall into two broad categories: technical information and business information. The lists below are not intended to be exhaustive or exclusive. Keep in mind that technical or business information falling under one of the classes listed below must still satisfy the other elements of a trade secret in order to meet the legal definition.

Technical Information
Trade secrets in this category may include:

- Plans, designs and patterns, such as those for specialized equipment
- Processes and formulas, such as those for the manufacture of drugs, foods, chemicals or other materials (*e.g.*, the formula for Coca-Cola)
- Methods and techniques for manufacturing
- Engineering notebooks
- Negative information, *e.g.*, the designs that *didn't* work (the UTSA definition of a trade secret "includes information that has commercial value from a negative viewpoint, for example the results of lengthy and expensive research which proves that a certain process will not work could be of great value to a competitor")
- Computer software (programs or source code)

Business Information
Trade secrets in this category may include:

- Financial information prior to public release
- Cost and pricing information
- Manufacturing information
- nternal market analyses or forecasts
- Customer lists
- Unannounced business relationships one is negotiating or has entered into
- Information about business opportunities, such as opportunities to acquire another company or product
- Marketing and advertising plans, both for existing and planned products
- Personnel information (*e.g.*, who the key employees are, what are the compensation plans for key employees, who would be a good target to hire away because of his or her special knowledge, experience, receptivity to solicitation, and the like)

Steps to Protect Trade Secrets

General Precautions
Trade secret owners have a duty to use "reasonable measures" to safeguard their secrecy. A common "reasonable measure" involves putting employees, contractors, vendors and other personnel on notice of the existence and nature of confidential information, and of a contractual duty on their part not to disclose it. Companies may include confidentiality provisions in form contracts, offer letters, requests for bids, and other appropriate documents.

Give workers (both employees and contractors) guidelines as to what sort of information the company considers confidential and how that information should be treated. Require them to sign non-disclosure agreements. Place warning labels on confidential documents and computer login screens. Issue periodic confidentiality reminders to workers as appropriate. In pursuing business opportunities, disclosures of trade secret information should occur under a license or non-disclosure agreement (itself a confidential document) that describes the information that is being disclosed; states the purpose(s) for the disclosure and the permitted exclusive use(s) of the information; and reiterates the other party's obligation to maintain the secrecy of the information. Vendors, suppliers, and independent contracting organizations or subcontractors should sign non-disclosure agreements at the inception of any relationship.

If an agreement is not possible, the trade secret owner should at least make clear its expectation that information is treated as confidential.

Although any protection measures must address specific risks applicable in that business and industry, extreme and unduly expensive procedures are not required. Beyond the obvious step of limiting access to confidential information to a "need to know" basis, following is a list of minimum practical "reasonable measures":

- Mark confidential documents and materials as such.
- Put locks on doors and file cabinets (or other forms of restricted access to physical files).
- Issue employee ID badges.
- Have specific procedures for visitors (signing in and out, visitor badges, no unescorted visitors).
- Require security passwords for computers and networks and limit access thereto.
- Provide a strong trade secret policy statement in employee handbooks.
- Have employees, contractors and third parties sign non-disclosure agreements.
- Do not discuss confidential information (including "hot projects") during interviews and limit tours of the facility (or have the applicant sign a nondisclosure agreement).
- Develop a matrix that classifies employees, consultants, contractors, and vendors according to the degree of access that they require and have been given to sensitive information.

You may find it necessary to take additional steps in specific areas, or with respect to specific kinds of information, such as limiting or monitoring the copying of documents or data in particular departments, prohibiting the removal or distribution of certain kinds of documents outside of a specific location, or prohibiting or limiting an employee from copying or working on company materials on their home computers.

Considerations in Recruiting Employees

- Instruct each person involved in the recruiting and hiring process not to use any confidential information belonging to his or her own former employers, and to use good judgment and caution when recruiting former co-workers from those employers.
- Similarly, do not use any proprietary information belonging to another business entity when seeking out and retaining independent contractors.
- New hires should be counseled not to bring with them or to use any information or materials belonging to another company, such as telephone directories, organizational

charts, salary schedules, and the like, as well as technical and business information that were protected as confidential by that company.

- If a current employee has signed a non-solicitation clause with his or her former employer, he or she may be prohibited from soliciting former co-workers to join him or her at your company. These non-solicitation agreements may be enforceable. If made in California, such agreements are enforceable only to the extent that they are necessary to protect the former employer's trade secrets.

- If a prospective employee has entered into a non-competition agreement with his or her current or former employer *outside of California*, that agreement may be enforced if it was lawful at the place and time it was made. You should question job applicants to find out whether they are bound by such an agreement and if so, ask to see a copy of it.

- Have applicants sign a statement confirming that they will not bring to their new job any confidential or proprietary information or trade secrets from their former employer, and that they will not reveal any such information either during the recruitment process or after being hired.

- In interviewing technical personnel in particular, interviewers should be careful not to "pump" an applicant for information about how his or her current employer conducts its business or the details of any of the employer's projects.

- Once applicants are far enough along in the interview process to be told specifics about the confidential operations of your company, have them sign a confidentiality agreement.

Considerations for Incumbent Personnel

- Once an employee is hired, he or she should sign a confidentiality and invention assignment agreement. Any incumbent employees who have not already signed such an agreement should sign one immediately as a condition of further employment. The employer may offer additional consideration such as a salary increase, promotion or bonus at the time the confidentiality agreement is signed in order to ensure there is adequate consideration for such an agreement from employees who are not at will.

- Consider having independent contractors sign confidentiality and invention assignment agreements that limit the kinds of other customers for whom they may work, both during and after the engagement. It may also be advisable to require them to agree to disclose identities of concurrent and future clients for a period of time after the contract ends.

- Make sure that incumbent employees and independent contractors are made aware and reminded of trade secret and confidentiality obligations through the dissemination of policy statements, memoranda and notices; the use of sign-on screens on computers and labels on binders and materials; and the promulgation of a confidentiality and trade secret policy, which should be made a part of the company employee handbook.

Considerations in Terminating Employees

One way in which businesses often try to protect their confidential information is by imposing non-competition agreements on departing employees and contractors. But in California and some other states, this option usually is not available. California's strong public policy against non-competition agreements is embodied in Business & Professions Code section 16600:

> Except as provided in this Chapter, every contract by which anyone is restrained from engaging in a lawful profession, trade or business of any kind is to that extent void.

Thus, the general policy in California is that an employer or contractor may not require an employee, subcontractor or vendor to sign a post-termination non-competition agreement.

The doctrine of inevitable disclosure, under which a trade secret owner may be able to enjoin the subsequent competitive employment of a former employee for a certain period of time, is not recognized in California because it offends this general policy, although it is recognized in some states.

In a non-solicitation agreement, one party agrees not to solicit or induce employees or customers (as the case may be) of the other party. Such agreements are generally executed between an employer and an outgoing employee (or between a principal and a departing contractor). The departing employee agrees that he or she will not solicit the former employer's remaining employees for the new employer, or solicit business from the former employer's customers (or both) for a specified amount of time. These agreements are usually enforceable, although in California they are only enforceable to the extent necessary to protect the former employer's trade secrets. If it appears that trade secrets are being used in the solicitation, the agreements can be enforced.

Protective measures a company should take upon the departure of an employee or independent contractor include:

- Give every departing employee and independent contractor an exit interview, during which the worker should return his or her access card, keys, passwords and the like. He or she should also return any documents or things in his or her possession, including things kept at home (such as company files on his or her home computer), in the car, as well as in his or her office or work area. In addition, disable the worker's access to voicemail, electronic mail, all computer access and access to other information and materials.
- During the exit interview, give the worker a copy of the confidentiality agreement that he or she signed upon joining the company, and remind him or her that the obligations under that agreement continue even after termination of employment or engagement.

- Conduct a review of the employee's or independent contractor's work area as part of the exit process. Have the worker point out and show the location of confidential materials that he or she usually worked with, including data on his or her computer. Usually the immediate manager is the person who best knows what that worker should or should not have in his or her possession and can be sure that everything is accounted for.
- Do not wipe the hard drive of any workstation, desktop or laptop of the departing worker that is being returned to the company's inventory without making sure that all files on the hard drive that need to be kept have been appropriately archived. After archiving, the hard drive should then be "wiped" so that no file can be resurrected. If the equipment is to be used by the departing worker's replacement, care should be taken to delete any departing worker's personal information that may be contained on the hard drive.
- Do not allow an employee or independent contractor in a sensitive position to stay on the job for any length of time after he or she has given notice of his or her intention to quit. Particularly if the worker is going to work in a similar or related industry, accept the resignation immediately and terminate the employment or engagement as soon thereafter as possible. This allows less opportunity for the worker to remove or pass along confidential data.
- After an employee or independent contractor has given notice, the company may monitor electronic mail access, as well as building access logs to determine if the worker has begun to come to the facility at odd times or has been staying in the facility for unusually extended periods of time. The company may also wish to monitor photocopying or the use of other office supplies that might indicate that the worker is copying data.

What Is Misappropriation?

Misappropriation does not need to be a deliberate act; it can occur through negligence or even mistake. "Misappropriation" is a statutory term that defines what one may not do with trade secrets one does not own. Section 3426.1(b) of the UTSA reads:

"Misappropriation" means:

(1) 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

(2) 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 or her 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 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.

This definition of misappropriation can be broken down into three types of prohibited conduct: (1) wrongful acquisition, (2) wrongful use, and (3) wrongful disclosure of someone else's trade secret. Each of these is discussed separately below. However, a common thread tying all of these concepts together is "improper means."

The UTSA expressly defines "improper means" to include "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means." The Comments to section 3426.1 provide a broader example: "Improper means could include *otherwise lawful* conduct which is improper under the circumstances; *e.g.*, an airplane overflight used as aerial reconnaissance to determine the competitor's plant layout during construction of the plant." Using authorized access to a network or computer system to obtain unauthorized access to information on the network or in the system would also be an example of "improper means."

Importantly, the plain language of the statute and the Comments emphasize that both reverse engineering and independent development are not misappropriation. The Committee notes define reverse engineering as "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." Additionally, the Comments provide that discovery of the trade secrets under license by the owner, observation of the purported trade secret in public use, or obtaining it from published literature are "proper means" and therefore not misappropriation.

Wrongful Acquisition

Misappropriation by wrongful acquisition occurs when all of the following conditions are met:

- The *acquisition* of a trade secret of another;
- By a person who *knows or has reason to know*; and

- That the trade secret was *acquired by improper means*.

A person who obtains by subterfuge or outright taking any information he has reason to know is confidential, is guilty of misappropriation. If a person obtains information directly or indirectly from someone who does not have authority to disseminate it, that person may be liable for misappropriation by wrongful acquisition.

Here are some examples of misappropriation by wrongful acquisition:

- Copying and removing trade secret documents from their storage location.
- Obtaining trade secret information from the trade secret owner's employee, if that employee had an obligation to maintain the information in confidence.
- Improper surveillance.

Similarly, the employer of an employee who wrongfully acquires and uses a trade secret on the job (*e.g.*, by bringing it from his or her old job) is liable to the trade secret owner for misappropriation and may also be subject to criminal penalties. See the discussion below.

Breaching or inducing another person to breach a duty to maintain confidentiality is another common problem. One who obtains confidential information, but *knows or has reason to know* that the source is under an obligation not to disclose such information, can be liable for misappropriation. The fact that a person under such an obligation willingly or accidentally disclosed the information *does not* protect the recipient.

Lawful acquisition of another's trade secrets, without more, is not actionable. The trade secret owner must show the defendant used "improper means" (discussed above) to acquire the information in order to show liability for this type of misappropriation.

Wrongful Use

Misappropriation by wrongful use occurs where:

(1) One *uses* the trade secret of another person;

(2) Without the express or implied *consent* of the owner of the trade secret; and *at least one* of the following is true:

(a) The trade secret was obtained by *improper means* (for example, you stole the information or employed other improper means to get it such as implanting and using a "backdoor" or "hook" in a computer program, system or network); or

(b) The trade secret was obtained from *another person who used improper means* to obtain it (for example, at the time of use, you knew or had reason to know that you got the information from or through a person who stole it, or used other improper means to obtain it); or

(c) The trade secret was obtained from *a person who had an obligation not to disclose it* (for example, at the time of use, you knew or had reason to know that you got the information from a person who was under an obligation–whether by a nondisclosure agreement or otherwise–not to disclose it to you); or

(d) You obtained the trade secret under an agreement or obligation *not to use it in the way you are using it* (for example, at the time of use, you knew or had reason to know that you learned of the trade secret pursuant to a nondisclosure or other similar agreement that prohibits the use you are making of the information); or

(e) You obtained the trade secret *knowing it was disclosed by accident* (for example, at the time of your use, but before a material change in your position, you knew or had reason to know that the information was dis closed to you by accident or mistake, such as by sending it to the wrong address, fax number or email account).

To prove misappropriation by wrongful use, a trade secret owner does not need to establish that the alleged misappropriator's product is an element-for-element copy of the owner's trade secret product or process. Proof of wrongful use is often made upon a finding of *substantial similarity* between the products or processes, or by inference. Example: at the end of its first month in business, Company A has only one customer that had not previously been a preferred customer of the trade secret owner, Company B. From this evidence, a court could infer that Company A did not acquire the names of B's customers through its own labor or public sources but rather, used Company B's trade secret customer list.

Wrongful Disclosure

The analysis of misappropriation by wrongful disclosure is virtually the same as that for wrongful use. Misappropriation by wrongful disclosure occurs when:

(1) One *discloses* the trade secret of another person to someone else;

(2) Without the express or implied *consent* of the owner of the trade secret; and *at least one* of the following is true:

(a) The trade secret was obtained by *improper means* (for example, you stole the information or employed other improper means to get it); or

(b) The trade secret was obtained from *another person who used improper means to obtain it* (for example, at the time you disclosed the information, you knew or had reason to know that you got the information from or through a person who stole it, or used other improper means to obtain it); or

(c) The trade secret was obtained from *a person who had an obligation not to disclose it* (for example, at the time you disclosed the information, you knew or had reason to know that you got the information from a person who was under an obligation–whether by non-disclosure agreement or otherwise–not to disclose it to you); or

(d) You obtained the trade secret under an agreement or obligation *not to use it in the way you are using it* (for example, at the time you disclosed the information, you knew or had reason to know that you obtained the secret information pursuant to a non-disclosure or other similar agreement that prohibits the use you are making of the information); or

(e) You obtained the trade secret *knowing it was disclosed by accident* (for example, at the time you disclosed the information, *but before a material change in your position*, you knew or had reason to know that the information was disclosed to you by accident or mistake, such as by sending it to the wrong address, fax number or email account).

Wrongful disclosure may be either intentional or inadvertent; the UTSA does not require "intent" to impose civil liability. A common example of misappropriation by wrongful disclosure occurs when a trade secret owner's employee has an interview with (or is actually employed by) a new employer, and discusses the former employer's trade secret information. Such an employee may be liable for misappropriation by wrongful disclosure, and the new employer may also be liable for misappropriation by wrongful acquisition and/or use.

Loss of Trade Secret Status and Other Defenses

Trade secret status may be lost over time. For example, new technology developed today may become generally known and quite common in a span of time as short as six months. If so, that information likely would no longer qualify as a trade secret. Similarly, after previously secret business information (such as bids, prices, or demand data) is released or otherwise becomes generally known, it loses any trade secret protection that it might have enjoyed.

Trade secret rights can also be lost through publication of the information, including the posting of confidential information via modern mass communications systems, such as the Internet or intranets. Anonymous postings, even if available for only a very short period of time, can destroy trade secret status because millions of people could have accessed the information even if few people in fact saw it.

Readily Ascertainable Information

The fact that information is "readily ascertainable" is an affirmative defense to misappropriation in California. In other words, if the trade secret owner presents evidence that the information at issue is not generally known, the defendant may show that the alleged trade secret information is readily ascertainable by proper means, such as availability in trade journals, reference books, or published materials.

Other "proper means" of ascertaining allegedly trade secret information include:

- Discovery by independent invention. However, this must be actual independent discovery, and not the mere possibility of it.
- Discovery by "reverse engineering," "decompiling" and/or "disassembly" (that is, by starting with the known product and working backward to find the method by which it was developed, provided, of course, that the acquisition of the known product was itself fair and honest, such as by purchase of the product on the open market). However, note that in cases where the reverse engineering is very time intensive and expensive, the information yielded is likely not to be considered "readily ascertainable" and would therefore still be a trade secret.
- Discovery under a license from the owner (assuming, of course, that the license does not include a confidentiality or nondisclosure agreement).
- Observation of the item in public use or on public display.
- Obtaining the information from published literature.
- Obtaining the information from one who is not under any obligation to keep it confidential (*e.g.*, obtaining a competitor's pricing from a mutual customer).

Remedies

Civil

The UTSA provides an extensive list of civil remedies for trade secret misappropriation, both in the form of monetary damages and injunctive relief. Trade secret owners may:

- Obtain an injunction prohibiting the actual or threatened misappropriation (Cal. Civ. Code § 3426.2).

- Recover compensatory damages for actual loss caused by the misappropriation (Cal. Civ. Code § 3426.3(a)).
- Recover compensatory damages for the defendant's unjust enrichment, to the extent not covered by the calculation of damages for actual loss (Cal. Civ. Code § 3426.3(a)).
- Obtain payment from the defendant of a reasonable royalty, if neither the damages nor the unjust enrichment caused by the misappropriation are provable (Cal. Civ. Code § 3426.3(b)).
- Recover exemplary (punitive) damages not exceeding twice the compensatory damages award if the misappropriation is "willful and malicious" (Cal. Civ. Code § 3426.3(c)).
- Recover attorneys' fees for bad faith tactics in trade secret litigation or willful and malicious misappropriation (Cal. Civ. Code § 3426.4).

Furthermore, the California Business and Professions Code § 17200 prohibits "any unlawful, unfair or fraudulent business act or practice." This statute is extremely broad in its coverage of prohibited acts and practices, and it creates a private right of action for redress of any practice forbidden by any other law (civil, criminal, federal, state, municipal, statutory, regulatory or court made). "Unfair" has been defined as any act or practice whose harm to the victim outweighs its benefits to the actor. This statute may allow a trade secret owner to bring a claim of unfair competition based on misappropriation of its trade secret. Section 17200 suits may seek injunctive relief or restitution but not compensatory damages.

Common law unfair competition claims can be used to impose liability for improper use of confidential information. Unlike claims under Section 17200, compensatory and punitive damages as well as injunctive relief are available for such claims.

Criminal

Numerous state and federal criminal statutes directly or indirectly prohibit trade secret misappropriation.

Cal. Penal Code § 499c
Theft of Trade Secrets

This statute's definition of a trade secret conforms to the UTSA. It subjects trade secret misappropriators (and persons conspiring with them) to criminal penalties if they appropriate trade secrets by wrongful or dishonest means, or if they offer anyone a bribe to do so. Intent to deprive, withhold or misappropriate information for one's own use or the use of another must be shown for criminal liability. A violation is punishable by a fine of up to $5,000.00, imprisonment of up to one year, or both. The violation can be either a misdemeanor or a felony, depending on the value of the trade secret stolen.

Cal. Penal Code § 496
Receiving Stolen Property

This statute makes it a crime to acquire or conceal property known to be stolen. The elements are simple: (1) the property must be stolen; (2) the defendant must have known the property was stolen; and (3) the defendant must have had possession of the stolen property. This statute can be used to prosecute persons who buy or otherwise receive trade secret information that they know was stolen. A violation is punishable by imprisonment of up to one year, and can be a misdemeanor or a felony depending on the value of the trade secret at issue. Under Penal Code § 496(c), the injured party may also bring an action for treble damages, costs and attorneys' fees (however, a defendant may argue the UTSA preempts this provision; the outcome would depend on the particular facts and circumstances).

Cal. Penal Code § 502
Unauthorized Access to Computers

This statute makes it a crime to gain access to and use any computer data or other computer hardware or software without authorization. Punishment for a violation ranges from a fine of $5,000 and/or up to one-year imprisonment to a fine of $10,000 and/or up to three years imprisonment. Also, any hardware or software used to commit the crime is subject to forfeiture. If the trade secret at issue is in the form of computer data, software or hardware, this statute may apply.

18 U.S.C. §§ 1831-39
The Economic Espionage Act

This statute is aimed specifically at trade secret misappropriation and contains provisions similar to Cal. Penal Code § 499c (including a definition of "trade secret" that coincides with that of the UTSA). Section 1832 addresses the theft of trade secrets generally (as opposed to "economic espionage," *i.e.*, the theft of trade secrets for the benefit of foreign governments, addressed in section 1831). Section 1832 requires proof of the defendant's "intent to convert a trade secret," and the fact that the trade secret at issue is "related to or included in a product that is produced for or placed in interstate or foreign commerce." The latter requirement casts some doubt on whether trade secret information that is *not* "related to or included in a product" is covered by the statute. An argument could be made that this law does not punish thefts of pure research information or service-related data, for example.

Punishment for violation is a fine of up to $250,000 (18 U.S.C. § 3571), imprisonment for up to 10 years, or both. "Organizations" (including business entities) convicted under this statute face fines of up to $5 million. Section 1834 also allows the court, in addition to the sentence imposed, to order violators to forfeit to the United States any property or proceeds resulting from the violation or used in connection with the violation.

18 U.S.C. § 1030
The "Computer Crimes" Statute

This statute does not expressly deal with trade secrets, but it does criminalize the use of computers during the course of other criminal activities (particularly during the conduct of otherwise fraudulent actions). One provision is of particular interest: section 1030(a)(5) makes it a crime to knowingly transmit a program, information, code or command with the intent thereby to cause unauthorized damage to another computer (or otherwise intentionally to access another computer without authorization and thereby cause damage). This provision criminalizes many activities, such as the transmission of computer viruses and so-called software "time bombs" (*i.e.*, bits of code that can be used to disable software programs at a preset time or date). Violations are punishable by fines of up to $250,000 (18 U.S.C. § 3571), imprisonment for one to 20 years, or both.

18 U.S.C. §§ 1341, 1343
Mail and Wire Fraud

Sections 1341 and 1343 prohibit schemes to defraud or obtain money or other property by false or fraudulent pretenses via use of the United States Postal Service (mail fraud) or wire, radio or television communications, or writings, signs, signals, pictures or sounds (wire fraud). Trade secrets and other confidential information qualify as "property" under these statutes. Punishment for violations of these statutes is a fine of up to $250,000 (18 U.S.C. § 3571), imprisonment for up to five years, or both. Because these statutes define elements of a crime that are easier to prove than those under the Economic Espionage Act, federal prosecutors may often decide to prosecute a trade secrets case under the mail and wire fraud statutes.

18 U.S.C. §§ 1961-68
RICO

The federal Racketeer Influenced and Corrupt Organizations Act ("RICO") allows the federal government to bring criminal complaints and indictments alleging that the theft of trade secrets constitutes the forming of an "enterprise" to engage in "a pattern of racketeering activity." A RICO violation requires continuity of the illegal conduct; in other words, a single act of trade secret theft may not be enough. Punishment for violation is a fine of up to $250,000 (18 U.S.C. § 3571), imprisonment for up to 20 years, or both, plus forfeiture of all

proceeds of the racketeering activity. The injured party may also bring a civil action for treble damages, attorneys' fees and costs.

18 U.S.C. §§ 2311-33
The National Stolen Property Act

This federal statute, similar in content to Cal. Penal Code § 496, prohibits (among other things) the receipt, sale or transportation in interstate or foreign commerce stolen "goods, wares, merchandise, securities or money, of the value of $5,000 or more." Based on a view that stolen trade secrets are "goods, wares, [or] merchandise," this statute can apply to trade secret theft (assuming the value of the information is at least $5,000).

A critical issue under this statute is whether the trade secrets must be embodied in some physical form, or whether mere electronic transmission of trade secret data would qualify as an offense under the statute. A violation is punishable by fines of up to $250,000 (18 U.S.C. § 3571), imprisonment of up to 10 years, or both.

18 U.S.C. § 1029
Fraud in Connection with Access Device

This federal statute criminalizes many activities performed with counterfeit or unauthorized "access devices," defined as "any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)."
In particular, it is a crime to use a counterfeit or unauthorized access device to obtain money, goods, services or any other thing of value. 18 U.S.C. § 1029(a), (e)(1). If a trade secret (by definition a "thing of value") were obtained in this way, this statute could apply. Punishment for a violation is a fine of at least twice the value of the thing obtained (or $250,000, whichever is greater), imprisonment of up to 20 years, or both.

Choosing Between Civil and Criminal
Because of the variety of criminal remedies for trade secret misappropriation, trade secrets owners are often interested in pursuing them. Some advantages do exist. The government bears the cost of investigation, discovery and prosecution. Governmental authorities can issue a search warrant and often can recover stolen trade secrets. The government may obtain evidence usable in subsequent civil actions. Finally, criminal cases are often disposed of more quickly than civil cases because of the constitutional requirement of a speedy trial. But there are at least an equal number of disadvantages. Once the government gets involved, the trade secret owner loses control over how, or even if, the case is prosecuted.

Government authorities are often overburdened and may have limited resources especially in cases where complicated technical data are involved.

Criminal cases will often delay civil cases; for example, civil defendants will move for a stay and/or refuse to testify on Fifth Amendment grounds. The prosecutor faces a much higher burden of proof in a criminal case (beyond a reasonable doubt, as opposed to the preponderance of evidence standard in civil cases). Once charges have been brought, the trade secret owner becomes a witness and will likely be subject to a subpoena to testify at a preliminary hearing and trial.

Depending on the circumstances, a criminal prosecution can have an adverse impact on the trade secret owner's public relations. A criminal conviction could have the effect of canceling the defendant's insurance coverage in the civil case.

Finally, perhaps the most important consideration of all to the trade secret owner, the trade secret information may become a part of the public record in a criminal proceeding because confidentiality concerns are likely to be outweighed by the defendant's constitutional right to examine the evidence against him. However, trade secret owners should take note of the fact that in civil cases, Cal. Code of Civil Procedure § 2019(d) requires a plaintiff asserting trade secret misappropriation claims to identify its alleged trade secrets with "reasonable particularity" before it is entitled to any discovery from the defendant relating to the allegedly misappropriated trade secrets. Any litigation, civil or criminal, brings with it the risk of unwanted disclosure of a party's trade secrets.

A trade secret owner should consult with experienced counsel and make a careful balance of the advantages and disadvantages of criminal remedies before deciding to involve criminal authorities in a trade secrets matter.

www.fenwick.com

Lawyers who get IT.™