From Orange County Lawyer Magazine, October 2010 Vol. 52 No. 10, Page 10

Confidentiality Agreements—What Every Business Lawyer Should Know

by Daniel S. Beebe

Use of Confidentiality Agreements, also commonly referred to as Non-Disclosure Agreements, Proprietary Information Agreements, or similarly titled documents, are primarily based in trade secret law which recognizes that a business has an ownership interest in and right to protect information it creates, from which it or others could derive some "economic value." Trade secrets have often been grouped together with patents, copyrights, and trademarks under the broad umbrella of intellectual property law and generally thought to be the exclusive domain of intellectual property lawyers. However, since the exchange and protection of confidential information is so central to every company's business activities, the application of trade secret law often intersects with other practice areas such as corporate, transactional, compliance, employment, and litigation.

Competitive Intelligence or Trade Secret?

At one end of the spectrum of business information is competitive intelligence which can be generally defined as "gathering, analyzing, and distributing Intelligence about customers, competitors and their products, and just about any aspect of the business environment needed to support executives and managers in making strategic decisions for their business organization." At the other end of the spectrum of business information are trade secrets, which can be broadly defined as "exclusive knowledge or information, generated by the labors of a business, having economic value in that it is unknown to others and gives the owner an advantage in its business activities." Depending on the business or industry the form of what is considered trade secret information can be somewhat variable, ranging from business, financial and marketing plans to technical data, future product plans, or information on strategic partnerships and customer lists. While obtaining and using competitive intelligence is an ethical and legal business practice, the line between information described as competitive intelligence and trade secret information is becoming increasingly blurred. To better educate business stakeholders on the difference between what is considered competitive intelligence as opposed to trade secret information, a review of the legal definition of "trade secret" is warranted. In the U.S., trade secret law is a creature of state law and, thus, varies somewhat by state. The majority of states have adopted some version of The Uniform Trade Secrets Act (UTSA), while others utilize the application of common law rules to define trade secret rights and remedies. The UTSA is a model law drafted by the National Conference of Commissioners on Uniform State Laws to more uniformly define the rights and remedies of common law trade secrets. Presently, forty-six states (plus the District of Columbia) have adopted some version of the UTSA. California, which adopted the UTSA without significant change, uses the following definition: "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) 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 (ii) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." *California Civil Code* §3426.1(d). A violation of California's version of the UTSA may entitle the injured party to injunctive relief, recovery of damages for the actual loss caused by

misappropriation, recovery for unjust enrichment caused by misappropriation that is not taken into account in computing damages for actual loss. If neither damages nor unjust enrichment caused by misappropriation are provable, the court may order payment of a reasonable royalty for no longer than the period of time the use could have been prohibited and if willful and malicious misappropriation exists, the court may award exemplary damages.

It should be noted that while federal law generally does not preempt or apply to state law claims involving trade secrets, there is federal law governing trade secret theft in the form of the Economic Espionage Act of 1996, *18 U.S.C.* §§1831-1839. The Economic Espionage Act (EEA) makes the theft or misappropriation of a trade secret a federal "crime" (including conspiracy to misappropriate trade secrets and the subsequent acquisition of such misappropriated trade secrets) with the knowledge or intent that the theft will benefit a foreign power or where misappropriated trade secrets are used in a product that is produced for or placed in interstate (including international) commerce and is done so with the knowledge or intent that the misappropriation will injure the owner of the trade secret. Penalties for violation of the EEA are fines of up to US $500,000 per offense and imprisonment of up to 15 years for individuals, and fines of up to US $10 million for organizations.

Although it is clear that state law governs trade secret protection except in the narrow areas of theft, misappropriation, or unauthorized use and possession of trade secrets related to products placed in interstate or foreign commerce or economic espionage for the benefit of a foreign company, agent, or government—it is important to recognize the EEA adopts a definition of "trade secret" consistent with the generally accepted legal definitions used in the UTSA and state laws based on the UTSA. Specifically, the EEA 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 public." *18 U.S.C.* §1839(3)

Harmonizing Use of Confidentiality Agreements and Trade Secret Protection

To the casual observer the disclosure of any trade secret information to another party would seem to destroy the trade secret status of such information. However, the law has long recognized the needs of businesses and individuals to exchange or disclose confidential information in furtherance of their business objectives, while protecting the rights of those businesses or individuals from having third parties economically benefit from use information they were not intended to receive or possess. Thus, providing confidential information to another party on a restricted basis and prohibiting further disclosure to any unauthorized third party are considered "reasonable measures" in maintaining the secrecy of such information. There are various methods companies can use to protect their trade secret information, such as: keeping the information in locked drawers, cabinets, or rooms; marking documents as confidential or secret; encrypting documents; or protecting computer files and directories with passwords, however, use of confidentiality agreements with business partners as well as employees is the primary method in which a business can demonstrate its reasonable measures to maintain the secrecy of its trade secret information. Several courts have held that use of confidentiality agreements constitutes

reasonable steps to ensure secrecy of the information for trade secret protection. *See American Credit Indemnity Co. v. Sacks*, 213 Cal.App.3rd 622 (1989), *Rockwell Graphic Sys., Inc. v. DEV Industries, Inc.,* 925 F.2d 174 (7th Cir. 1991), *On-Line Communication Servs., Inc.*, 923 F.Supp. 1231 (N.D.Cal. 1995).

Confidentiality Agreements as Contracts

While the use of Confidentiality Agreements is based on the "reasonable efforts to maintain its secrecy" language in both the state and federal statutory definitions pertaining to trade secrets, it is important to understand that use of Confidentiality Agreements is equally based in contract law. Parties are generally free via contract to define the terms regarding the purpose of the agreement, the description of the confidential information being disclosed, the period of protection for such confidential information, or even negotiate the state law that will govern interpretation of the agreement. *California Civil Code* §3426 clearly recognizes that a party may have a cause of action in breach of contract for violation of the terms of a Confidentiality Agreement: "(b) This title does not affect (1) contractual remedies, whether or not based upon misappropriation of a trade secret, (2) other civil remedies that are not based upon misappropriation of a trade secret." *California Civil Code* §3426.7(b). Further, while §3426 limits remedy to "damages for the actual loss caused by misappropriation . . . [or], If neither damages nor unjust enrichment caused by misappropriation are provable, the court may order payment of a reasonable royalty for no longer than the period of time the use could have been prohibited," however, liability for breach of contract damages is not so limited.

A California case which best illustrates the importance of contract provisions in a Confidentiality Agreement is Celeritas Technologies, Ltd. v. Rockwell International Corporation. In the early 1990s representatives of Celeritas met with members of Rockwell to demonstrate Celeritas' proprietary de-emphasis technology applicable to modem semiconductor chips—Rockwell was a leading modem chip manufacturer at the time. The parties entered into a non-disclosure agreement (NDA), which covered the subject matter of the meeting. In 1994, a Rockwell competitor began to sell a modem product that incorporated de-emphasis technology and Rockwell subsequently informed Celeritas that it would not license the use of Celeritas' proprietary technology. Rockwell soon thereafter began efforts to develop de-emphasis technology for its modem products, shipping its first prototype de-emphasis technology chip sets in January 1995. In September 1995, Celeritas sued Rockwell, alleging breach of contract, misappropriation of trade secrets, and patent infringement. At trial, Celeritas prevailed under all three theories, however, on appeal the patent infringement claim was dismissed and the misappropriation claim was rendered a duplicative recovery based on a Celeritas recovery stipulation at trial. Essentially, Celeritas' recovery was based on breach of the NDA provision where Rockwell covenanted not to use "any [Celeritas] Proprietary Information (or any derivative thereof) except for the purpose of evaluating [a] prospective business arrangement [with] Celeritas . . ." *Celeritas Technologies, Ltd. v. Rockwell International Corporation*, 150 F.3d 1354 (Fed.Cir. 1998). Final compensatory damages, based what it would have cost Rockwell to license the technology from Celeritas, together with exemplary damages awarded Celeritas under its breach of contract claim totaled approximately $65 million.

Confidentiality Agreements: Provisions to Include and Pitfalls to Avoid

While irrespective of any written agreement, a duty of confidentiality may exist at common law; it is highly recommended that the parties involved memorialize their obligations concerning

the use and protection of confidential information disclosed in an agreement between them in order to maximize protection and prevent misuse of their respective trade secret information. Many of the definitional provisions or provisions excepting certain information from trade secret status are the result of common law decisions, while others are based in the UTSA or EEA. Many other provisions that may be included in a Confidentiality Agreement, as noted above, are based in contract law and subject to negotiation between the parties. Below is a discussion of the more important issues to be considered when drafting and negotiating confidentiality agreements.

Definition of Confidential Information

A preferred practice in virtually every confidentiality agreement is for the parties to define what information is "confidential" as well as whether one or both parties are disclosing confidential information. Further, it is important to include a "marking" requirement which provides that "Information shall be considered confidential if provided to the receiving party in written or electronic form and marked as "confidential," "proprietary," or similar conspicuous legend, if provided orally or visually, is identified as confidential at the time of delivery and promptly confirmed as confidential in writing to the receiving party within, or which a reasonable person would not recognize from the surrounding facts or circumstances to be confidential or secret." However, any description which attempts to protect all intellectual property rights of the disclosing party should be avoided since any registered patented, copyrighted, or trademarked material are publically available for all to see and, thus, are not protectable as trade secrets.

Exceptions to Confidential Treatment

Confidentiality agreements typically exclude certain information from the definition of confidential information. A somewhat universal exception to a claim of trade secret protection is the "public domain" exception. As noted above, if the confidential information is or becomes available to the general public, except as the result of an unauthorized disclosure, then the information is no longer considered "secret." The seminal case on the issue, *Kewanee Oil Co. v. Bicron Corp.* held, "the disclosure of a trade secret, even if accidental or inadvertent, destroys the 'secrecy' and removes protection." *Kewanee Oil Co. v. Bicron Corp.,* 416 U.S. 470 (http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=416&invol=470), 476 (1974). Further, information already known to the receiving party prior to receipt and absent any confidentiality commitment on the part of the receiving party is another exception to trade secret status. Another common exception to trade secret status concerns information that a party, through its own labors, has developed "independently" of any relationship with the disclosing party. The legislative history of the EEA indicates such independent or "parallel" development is a clear exception to the trade secret protection under the EEA. *See* www.usdoj.gov/criminal/cybercrime/EEAleghist.htm (Managers' Statement for H.R. 3723). The last general exception to trade secret status is the "court order" exception. This is not a true exception to trade secret status but rather exception to the receiving party's obligation of non-disclosure to any third party. This exception provides that a the recipient of trade secret information cannot be held to be in violation of its confidentiality obligations if the receiving party is compelled by a subpoena, court order, or other request pursuant to legal process, to produce any of the disclosing party's trade secret information. Both California trade secret law the EEA contain language which supports this exception by requiring that courts take such actions as necessary to preserve the

confidentiality of the trade secret provided pursuant to court order. *See* 18 U.S.C. §1835 and California Civil Code §3426.5.

Term

One of the more important provisions to consider when negotiating a confidentiality agreement is its term. In other words, how long do the confidentiality and other obligations of an agreement last? Most businesspeople and many lawyers think of "term" as being a single fixed time period. But for most confidentiality agreements, there actually are two time periods to consider—the time period during which confidential information will be disclosed and the time period during which the confidentiality of the information is to be maintained. These periods may or may not be the same, and they need not be specified by exact dates (years, months, weeks, etc.). For example, the parties may provide that the term of the agreement shall continue for so long as the parties are discussing a possible business relationship, but the obligation of confidentiality survives until an exception to the obligation arises. Other agreements may quantify the time periods and, for example, provide that the disclosure period is for one year and the obligation to maintain the confidentiality of the information is for a three-year period thereafter. Time limits on protecting confidential information vary based on the sensitivity of the information being disclosed, with anywhere from three to five years being somewhat the norm. However, courts have been reluctant to enforce such provisions where the useful life of the trade secret has expired, i.e. "[t]he plaintiff must prove that . . . the trade secrets are not "stale" *See Computer Economics, Inc. v. Gartner Group, Inc.*, 50 F.Supp.2d 980, 984-92 (S.D.Cal. 1999). Lastly, the agreement should provide for termination by either party at any time, subject to reasonable notice as negotiated by the parties. This allows either party to terminate its participation under the agreement if it decides working with the other party is no longer in its business interests.

Obligation of Confidentiality

Every confidentiality agreement should detail how the confidential information will be handled by the recipient. The receiving party's failure to treat the confidential information in compliance with these requirements will result in a breach. At a minimum, the receiving party should be required to use the same amount of care in preserving the secrecy of the confidential information as used in preserving the secrecy of the receiving party's own Confidential Information, but in no event less than "reasonable care." Other typical requirements include restricting disclosure to only those employees who have a real "need to know" the information to evaluate the relationship; non-use of the confidential information for other than the specified purpose agreed to by the parties, and; no disclosure of the confidential information to persons or entities other than the employees or agents of the recipient without the prior written consent of the disclosing party. If employees, contractors, or agents of the recipient are provided access to the confidential information, the disclosing party should expressly provide in the agreement that the recipient must cause those persons to be bound by the same obligations of confidentiality as provided for in the agreement, while the receiving party will remain responsible for the acts of those persons in regard to the confidential information received.

Ownership and Warranties Regarding the Confidential Information

The disclosing party should also consider requiring the recipient to acknowledge that the confidential information is the property of the disclosing party and that the disclosure of the

information does not convey any right, title, or license in the information or rights to any patent, copyright, trademark, or any other intellectual property right of either party under the Agreement. This is necessary to prevent ambiguity as to what rights, if any, the recipient has in the confidential information and any information related thereto (i.e., no implied license). Further, it is always wise to insert a warranty or representation regarding the disclosing party's ownership of the confidential information or at a minimum that the disclosing party warrants that it has the right to disclose the confidential information provided under the agreement.

Return and/or Destruction of the Confidential Information

If the term of the agreement has expired or if the agreement is terminated pursuant to a termination provision, there is generally no purpose for the receiving party to continue to possess the disclosing party's confidential information. The preceding given, it is a recommended practice to insert a provision in the agreement that requires the receiving party, upon the disclosing party's written request, will promptly return all confidential information received from the disclosing party, together with all copies, recordings, summaries, or other reproductions thereof and all notes and/or other works prepared or based thereon, or certify in writing that all such confidential information and copies have been destroyed.

Prohibition on Reverse Engineering

Absent a license agreement or other agreement prohibiting such, once products are sold and are in the public domain, they may be freely reverse engineered to reveal any inherent trade secrets. Courts in the U.S. have treated reverse engineering as an important factor in spurring inventors to disclose innovations which benefit the general public rather than maintaining such inventions as trade secrets. A patent allows qualifying inventors up to 20 years of exclusive rights to make, use, and sell the invention, but only in exchange for disclosure of significant details about their inventions to the public. However, should the inventor choose to protect the invention as a trade secret, his or her competitive advantage may be short-lived if the innovation can be reverse engineered. Further, purchase of a product in the open market generally confers personal property rights in the product, including the right to take the product apart, measure it, subject it to testing, and the like. In fact, California trade-secrecy law explicitly provides that reverse engineering is a lawful way to acquire a trade secret, "[r]everse engineering or independent derivation alone shall not be considered improper means." Civ.Code, §3426.1, subd.(a). However, where non-publicly available prototypes, preproduction examples, beta, or pre-release code are being provided under a confidentiality agreement, a prohibition on reverse engineering of such prototypes or pre-production/pre-release products is not only warranted but highly recommended.

Right to Equitable Relief

In a situation where the trade secret is a key component of the business model and profitability of the company, it is quite possible that no amount of money damages would be adequate or preferable to enjoining the breaching party from continued misuse use of the owner's confidential information. For this reason, California law provides for injunctive relief against "[a]ctual or threatened misappropriation" of a trade secret, (Civ.Code, §3426.2) and courts are allowed this remedy (provided by statute) in granting an injunction against actual or threatened use of misappropriated trade secrets. *See Morlife, Inc. v. Perry,* 56 Cal.App.4th (1997). However, depending on the sensitivity of the information, the business lawyer should be on guard against

language which indicates the unauthorized use or disclosure "may" cause irreparable harm and that the injured party may be entitled to "seek" equitable relief—since the burden of proof still remains with the complaining party to show the harm caused cannot be satisfied by monetary damages and equitable relief is not a "right" under the agreement.

Consequential Damages Disclaimers and Other Damages Limitations

Many companies attempt to limit their liability for any perceived or actual misuse of confidential information received by inserting a disclaimer of consequential or other indirect, special, or punitive damages. The business law practitioner who encounters such a provision should take note that while there is a specific provision for "exemplary damages" (similar to punitive damages) in California Civil Code §3426.3, the parties are free to negotiate a limitation on these damages via contract and such disclaimers or limitations are generally enforceable. However, it should be noted that consequential damages disclaimers tend to limit any real contractual damages remedy that could be pursued since the injured party is limited to recovery of only direct damages incurred which under a confidentiality agreement are difficult to prove. Some parties attempt to use a liquidated damages clause setting forth the damages the owner of such confidential information might be entitled to in the event of a breach of the agreement. As with consequential damages disclaimers noted above, liquidated damages clauses in confidentiality agreement are also enforceable, however, the inclusion of such a provision may eviscerate any clause providing for injunctive relief. Since granting an injunction is generally disfavored by courts where money damages would suffice to remedy the situation—inclusion of a liquidated damages provision would likely be viewed by a court as tantamount to saying money damages "would" suffice—and may result in injunctive relief being denied.

Exclusion for Commonly Used Skills, Know-How and Residual Memory Clauses

The EEA clearly recognizes that trade secret information can be misused or misappropriated by both tangible and intangible means, i.e., memorization, ". . . all forms and types of financial, business, scientific, technical, economic, or engineering information, . . . whether tangible or intangible, and whether or how stored." 18 U.S.C. §1839(3). The statute also prohibits transcribing such intangible, memorized information into a tangible form, such as "sketch[ing], draw[ing], . . . download[ing], upload[ing], . . . , transmit[ting], . . . communicat[ing], [and] convey[ing]," 18 U.S.C. §§1831(a)(2), 1832(a)(2). This is not to say, however, that any piece of business information that can be memorized is a trade secret. The EEA does not apply to individuals who seek to capitalize on their lawfully developed knowledge, skill, or abilities, nor does the EEA apply to individuals who merely have been exposed to trade-secret information. However, some states prevent the free movement of key employees who may "inevitably" disclose trade secret information of their former employers. The "Inevitable Disclosure Doctrine" is the law in states such as Illinois and Colorado and is a method of proving a misappropriation claim. It is based on the theory that certain key employees cannot resign and work for a competitor without inevitably using, in their new jobs, their former employer's trade secrets, even if they do not intend to. The typical remedy has been to enjoin a party from conducting business in the same or similar role until such time as information he or she possesses becomes stale. The leading inevitable disclosure case is *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262 (7th Cir. 1995). California courts on the other hand have in several cases rejected the inevitable disclosure doctrine as the law in California . *See Bayer Corporation v. Roche Molecular Systems,* Inc., 72 F.Supp.2d 1111, 1119 (N.D.Cal. 1999). While the foregoing exclusion of commonly

used skills, know-how, or talent is usually more applicable in an employee form of confidentiality agreement, the same principle has been held applicable in confidentiality agreements with other business partners, such as sales representatives or agents. For example, one court has held that a terminated agent cannot be prohibited from using skills that he or she acquired, or casually remembered information that he or she acquired, while employed by the principal. *Apollo Techs. Corp. v. Centrosphere Indus. Corp.*, 805 F.Supp. 1157, 1200 (D.N.J. 1992).

To avoid claims that their employees are tainted merely by being exposed to another party's confidential information, many large companies attempt to insert what is referred to as a "residual memory clause." Residual memory clauses generally provide that the receiving party has a right to use any confidential information retained in the unaided memories of their employees who had access to the information. The argument used for inclusion of a residuals clause by such companies is that its employees cannot "un-remember" what they have seen or been exposed to and, thus, absent a residuals clause, any similar development efforts might become contaminated by an exposed employee's continued involvement. While the EEA expressly recognizes that trade secrets may be misappropriated by "memorization"; trade secret cases that do not involve the EEA are not persuasive authority on residual memory clauses or differentiating between intentional memorization and unintentional memorization. Companies that fear their confidential information may "memorized" by their business partners should insert language in the agreement which requires the return or destruction of the confidential information as well establishing limited access to named individuals of the receiving party who have an absolute need to access the confidential information solely for the purpose set forth in the agreement.

Non-Solicitation and Non-Compete Clauses

It is not uncommon to see non-solicitation clauses as part of a confidentiality agreement where the recipient agrees not to solicit for employment employees of the disclosing party or in an employment context, the employee agrees not to solicit the business of his or her employer's customers or solicit/recruit former co-workers for employment for some period of time after the employment relationship is terminated. California courts have enforced non-solicitation provisions barring business partners from soliciting or dealing directly with specifically named parties (*see General Commercial Packaging, Inc. v. TPS Package Eng., Inc.*, 126 F.3d 1131 (9th Cir. 1997)) or barring ex-employees from soliciting customers where the customer identities specific information regarding the customers which are trade secrets. *See Courtesy Temporary Service, Inc. v. Camacho*, 222 Cal.App.3d 1278 (1990). While reasonably constructed non-solicitation clauses are enforceable, contractual bans on competition in confidentiality agreements, especially within an employer-employee arrangements are not generally enforceable in various jurisdictions as being an unreasonable restraint on trade. These restrictive covenants generally seek to prevent a business partner from working on a similar project with a competitor of the disclosing party or seek to prohibit an employee from taking the same or similar position with a competitor of the employer after the employment relationship has ended. In California, Cal.Bus.&Prof.Code §16600 provides that, in the absence of a statutory exception, "every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void." A party operating in California seeking to limit its business partners from engaging in lawful business by inclusion of a non-compete clause or an employer

that insists on an employee's agreement to such covenants as a condition of employment may very well face liability under unfair competition theories.

Conclusion

While many business people routinely use confidentiality agreements to accomplish their day-to-day business activities, many fail to understand the real need and importance of confidentiality agreements in not only protecting the competitive edge the company may have in its confidential information but in also helping the company avoid liability by documenting the obligations of each party relative to the information he or she may receive. To better educate clients on the importance of confidentiality agreements, the business lawyer should recommend the use of a company-approved confidentiality agreement which should be part of the business' confidential information or information security policy, or absent a separate confidential information policy the importance of protecting confidential information should be stressed in the company's code of conduct, employee handbook, or intellectual property policies. Bottom-line, businesses that fail to understand the measures necessary to adequately protect their confidential information as well as the obligations for management and employees regarding use and protection of information they may receive or obtain from others may very well see those practices reflected in their "bottom-line."

Daniel S. Beebe is a solo practitioner focusing on in-house legal consulting, transactional matters, and intellectual property licensing. Mr. Beebe maybe contacted via email at daniel_beebe@yahoo.com ; and web at http://www.linkedin.com/pub/daniel-beebe-esq/0/4a9/32a.