A Practitioner’s Guide to Confidentiality Agreements
by Jere M. Webb

Introduction

Confidentiality agreements have become pervasive. As a result of the “high-tech” revolution, the short life span of new technology and products, and the perceived inadequacies of patent and copyright protection, in recent years there has been an exponential increase in the use of trade secret principles to protect technology or confidential information. As a result, virtually every employee of a technology-related company, and many consultants, independent contractors, licensees, partners, and joint ventures, have signed confidentiality agreements. Such agreements are also widely in use outside the high tech field to protect confidential business information, such as customer lists, marketing plans, and financial data. Once the narrow province of intellectual property lawyers, these agreements have come into the mainstream of legal practice. Their use by laymen and lawyers alike often is marked by a lack of knowledge of their intricacies and risks; thus, we will analyze the principal elements of such agreements both from the point of view of the owner of confidential information and from the point of view of the recipient.

Confidentiality agreements travel under a variety of names. They may be called “non-disclosure agreements,” or “trade secret agreements,” or “technology protection agreements.” Confidentiality covenants may be tucked away in agreements which have a broader purpose, such as employment agreements, technology transfer or licensing agreements, and a variety of others.

I. Advantages of Using Confidentiality Agreements

Most states will protect trade secrets from unauthorized use or disclosure by employees and others who “stand in a confidential relationship” with the owner of the information. However, without a written agreement, one is much more subject to the whims of judges and juries and to the vagaries of common law rules applicable to protection of trade secrets. For instance, some courts will not assume that a confidential relationship exists with a low level employee.1 Similarly, the owner is much more likely to obtain relief if the parties have agreed ahead of time that certain information constitutes trade secret or proprietary information of the party disclosing it.2

Finally, such agreements need not be limited to trade secrets; that is, secrets which give a commercial advantage. As one early expert has noted, “It matters not in such cases whether the secrets are secrets of trade or secrets of title or any other secrets of the party important to its interest.”3 Using a written agreement is advisable also because it allows the parties to tailor their rights and responsibilities to the particular circumstances involved and to provide for normal contract contingencies, such as dispute resolution.

Noncontractual methods of protecting trade secrets are beyond the scope of this article. However, the importance of having a general trade secret protection program should not be overlooked. Courts are not likely to protect as a trade secret something which the owner has failed to treat as confidential. This is particularly true where the contract uses only a general description of what is protected. The owner’s practice often will influence the court’s decision as to what was intended to be covered.

Mr. Webb is a partner in the firm of Stoel Rives LLP in Portland, Oregon.

© Stoel Rives LLP
II. Risks Associated with Receipt of Confidential Information

Having access to confidential information owned by another is not an unmitigated blessing; significant risks are involved. Since trade secret status may be lost forever by any disclosure of the secret, there is a constant threat of litigation should the secret unintentionally fall into the public domain. Ask, for instance, whether you would want to be trusted with the formula for COCA COLA (that is, the “classic” version) or, more pertinently, whether you would want it entrusted to one of your employees. For this reason, many companies have a policy of refusing to sign confidentiality agreements and of refusing to receive confidential information without a disclaimer of liability.

A common mistake made by persons who are asked to sign a confidentiality agreement is to assume that liability will arise only in the event of intentional disclosure. Since intentional disclosure is subject to control, the risk is deemed to be low. This is often not true. Liability will almost certainly exist for negligent disclosure, and the standard of care may be quite high either by reason of the existence of a fiduciary or quasi-fiduciary relationship or by reason of having been placed on notice of the valuable nature of the information and the irreparable harm which would follow from disclosure.

Furthermore, many confidentiality agreements impose a simple contractual obligation to keep secret information confidential. This obligation is not based upon the existence or non-existence of negligence; like most covenants, it imposes liability without fault. In representing the recipient of confidential information, consideration should be given to limiting the obligation to one of exercising reasonable care or of complying with certain delineated standards. The recipient may also wish to limit the remedy available in the event of breach or provide that any loss will be funded by insurance. Curiously, one rarely sees confidentiality agreements which contain such limitations.

III. Preliminary Discussion Agreements

A frequent mistake in dealing with confidential information is to neglect protection during preliminary discussions which could lead to preparation of a formal agreement containing confidentiality obligations. The discussions may be preliminary to sale of a business, arrangements for manufacturing a product, joint marketing of technology, technology licensing or transfer, employment arrangements, and a variety of other situations where it may be difficult, if not impossible, to conduct the discussions without at least some disclosure of confidential information.

Although common law principles may imply promises of nondisclosure or nonuse in such circumstances and, although oral promises of nondisclosure may be made, reliance on these avenue of protection is inadvisable. The rule of thumb should be that no confidential information will ever be disclosed without a written agreement, even if it is just a one-paragraph letter agreement.4

IV. Definition of Confidential Information

One of the principal problems in preparing a confidentiality agreement is defining the subject matter. There are three basic approaches: (1) general description; (2) specific description; and (3) marked items. There are advantages and disadvantages to each approach.

A. General Description

The most common approach is to define the subject matter generally such as: “I agree not to use or disclose any trade secrets or confidential or proprietary information of XYZ Company.” This approach is easy to draft, arguably gives the broadest protection because virtually anything which falls into the description will be covered, and solves the problem of future or unanticipated items.

The disadvantages are that it is vague and difficult to apply to concrete situations. This generates both legal and practical risks. On a
practical level it is clear that a recipient of confidential information is more likely to satisfy his obligations of nonuse and nondisclosure if the information is specifically defined. On a legal level the lack of a specific definition means an increased risk of disputes as to what is covered by the agreement. There is even some risk that the clause will be held to be so indefinite as to be unenforceable. By attempting to sweep broadly one could end up with no protection at all.

Although agreements are getting more detailed as companies gain sophistication and as use of trade secret concepts spreads, the general description approach to the definition problem probably is still the one most commonly used.

B. Specific Description

The next most common approach is to define either in the body of the agreement or, if the identification is lengthy or will change over time or will vary depending upon the person signing the agreement, in an exhibit attached to the agreement. This method tends to be used by companies which have sophisticated technology protection programs. They are likely to be able to identify their trade secrets with some particularity and usually they do not want to risk limiting the protection of items which they value most be combining them with items which may or may not qualify for protection.

Where confidential information can be specifically identified, it should be, at least in cases where the owner is sure that disclosures will be limited to the identified material. More likely, however, the subject will be more general, such that it is difficult to capture in words, or the owner will want to protect against disclosure of information not presently contemplated or perhaps not yet in existence. In these situations, one of the other approaches should be employed.

C. Marked Items

Limiting the nondisclosure obligation to marked items is a common approach and one which appears to be gaining in popularity. This approach removes almost all doubts about what is covered. It has limitations in situations where the confidential information is not reflected in written documents. Enforceability, however, is almost assured, at least in cases where the information is, in fact, confidential. Remember that with respect to use, if not nondisclosure, one cannot create trade secret status merely by marking an item as such. Unanticipated or future items are easily handled; one needs only to stamp them as “Confidential.” About the only disadvantage is that employees will forget to mark appropriate materials.

There is a middle ground between general description and specific description or marked items. The following language combines the three approaches and arguably garners the benefits of each. “As used in this agreement, ‘Confidential Information’ means (a) information identified in Exhibit A attached hereto; (b) any information marked by Company as confidential or otherwise identified as confidential; and (c) information treated by Company as confidential.” This approach takes care of the problem of mistaken failure to mark or designate and also may achieve the broadest scope of protection, provided that the owner, in fact, enforces its protection program.

V. Representing the Recipient of Confidential Information: The Exclusions Clause

In reviewing a confidentiality agreement as an information recipient, the exclusions clause will usually be the most important issue. Although the recipient may rely upon common law principles to provide protection against an overreaching confidentiality agreement or unanticipated occurrences, a well-drafted exclusions clause is much better. Most agreements exclude information which is or becomes part of the public domain. Several other exclusions should be considered.
A. Already Known

Information already known to a recipient should be excluded; otherwise the recipient may be precluded from using its own trade secrets or other information not considered part of the public domain. For instance, the prospective manufacturer of a product, before examining the details, may agree to nonuse (except for benefit of the owner) and nondisclosure of a “new” method of manufacturing. Thereafter the method is disclosed but turns out to be one which, although not generally known in the industry, is already known by the recipient and also by its principal competitor.

Another solution to the already-known information problem is to require the recipient to list in an attachment the inventions or trade secrets which will be excluded from operation of the confidentiality agreement. This method is often used in employment agreements with respect to the employee’s obligation to disclose and assign to the employer inventions made during the course of employment.

Individuals and representatives of small companies often will know from the general subject matter whether there is any chance that the information is already known. If there is no such risk, an exclusion of already-known information will be of little concern. This is less likely to be true, however, for large companies or for companies which deal in a wide range of technology products. In such cases an exclusion for already-known information is essential.

The problem with drafting this exclusion is that the owner of confidential information will not want to trust the recipient’s word that the information was already known. One solution to this problem is to provide that the information must have been reduced to writing by the recipient prior to disclosure by the owner.

B. Receipt from Third Party

Confidential information is often passed among a small group of persons and does not become part of the public domain. Following disclosure by the owner, the recipient may obtain the information from a third person under circumstances which involve no violation of the rights of the owner. In this event, the recipient should be free to use the information, as is true with information which becomes part of the public domain, or is already known, or is independently developed (see below), the recipient will want to make sure that he is not worse off by reason of having signed a confidentiality agreement. It is one thing not to be able to use certain information that no one else but the owner may use; it is something else to be excluded from using information that others may use, especially if the others are your competitors.

C. Independently Developed

Information independently developed by the recipient should be excluded from the confidentiality agreement for the same reasons as are applicable to the previously discussed exclusions. Like these other exclusions, there is the problem of documentation. The recipient will normally be happy with a generally worded exclusion, such as that suggested below. The owner, however, may wish to devise language which will make the exclusion operative with some verifiable documentation. The problem here is more troublesome than in the case of already-known information, in that it is difficult to exclude the possibility that the person who claims independent development had access to the disclosed information, and reference to the date of preparation of documentation does not always solve the problem. Usually the solution is to use a general exclusion, leaving the burden of proof on the person claiming independent development.

D. Suggested Exclusion

The following exclusion covers the points discussed above:

Notwithstanding the foregoing, recipient shall not be required to protect or hold in confidence, nor shall it be prevented from using, any information which (a) is or becomes part of the public domain; (b) is already known to recipient and has been reduced to writing by recipient prior to the date of this agreement; (c) is subsequently rightly received by recipient from a third party; or (d) is independently developed by recipient.
Faced with a recipient who demands that certain exclusions be added to the owner’s standard confidentiality agreement, the owner may wish to take steps to protect against fraudulent, improper, or mistaken invocation of the exclusions. One way to do this is by careful drafting of the conditions precedent (such as documentation) to operation of the exclusions. An alternative (or additional) method of protecting the owner is to place a special burden of proof on the recipient (beyond the normal “preponderance of the evidence”) with respect to any asserted exclusions. For instance, the exclusions clause might contain a provision such as the following:

In any dispute with respect to these exclusions, the burden of proof will be on recipient and such proof shall be by clear and convincing evidence.

VI. Restrictions on Recipients’ Employees

Where the recipient of confidential information is a legal entity, such as a corporation or partnership, consideration must be given to the fact that companies act through their employees and that the actual recipients of the confidential information will, therefore, be individual persons. The problem is what should be put in a confidentiality agreement to restrict such individuals. This problem is ignored in most form confidentiality agreements. Generally, three provisions are advisable. First, disclosure of the confidential information should be limited to designated employees or, if that is not practical, to “need to know” persons. Second, the confidentiality agreement should require that all individuals who receive confidential information be notified of its confidential character and that it is the subject of a confidentiality agreement between the employer and the owner of the information. Finally, it should require the employer to obligate each such employee to keep the information confidential.

The owner of confidential information may even wish to take the additional step of requiring the employer to have each employee sign a confidentiality agreement in specified form, with the form attached as an exhibit to the confidentiality agreement signed by the employer. Suggested language for this format is as follows:

Recipient agrees to obtain from its employees, prior to disclosure of confidential information, a signed employee confidentiality agreement in the form set forth in Exhibit A attached hereto.

This sort of provision is usually not necessary where the recipient is a company which regularly deal sin confidential information; such a company will already have obligated all appropriate employees to a general nondisclosure agreement which covers any information designated as confidential, whether owned by the company or by third parties. This is a step worth considering, however, in any case where doubt exists either as to the terms of the employer’s standard nondisclosure agreement or as to whether it has been signed by all employees who may come into contact with the subject confidential information.

VII. Assignment of Inventions

Where the employee participates in development of confidential business information, he may have some rights to the information under common law principles; indeed, the employee may be the exclusive owner of such information. Even where the employer owns the information, courts may be less generous in protecting the employer against use or disclosure of the information by a former employee where the employee was the source or creator of the information.6

The normal solution to this problem is an agreement providing that the employee will disclose and assign to the employer all inventions or trade secrets developed by the employee during the term of employment. However, as one expert has noted, “great care in drafting must be taken” because of the tendency of many courts to construe such agreements strictly against the employer.7 If there is any readily discernible path which leads to denying the invention to the employer, courts are likely to take it.8 Furthermore, several states have protected by statute the employee’s ownership of inventions which were not conceived or developed through use of the employer’s time, facilities or materials and which do not relate to the employer’s business.9
VIII. Liquidated Damages

Confidentiality agreements occasionally contain a liquidated damages clause: that is, a clause which provides that damages in a designated amount will be paid to the owner of the information should the confidentiality or other obligations of the agreement be breached. There are two problems with this type of clause. First, many states have stringent rules as to enforceability of liquidated damages clauses.10

Second, there is a school of thought which says that a liquidated damages clause in a confidentiality agreement may impair the ability to obtain an injunction in that it makes it more difficult to establish that there is no “adequate remedy at law.” One of the principal reasons for deeming the remedy at law inadequate is the difficulty of determining damages. If the parties themselves have determined the damages pursuant to a liquidated damages clause, this impediment is removed. The risk that inclusion of the clause would make it more difficult to obtain an injunction needs to be balanced against the obviously beneficial “in terrorem” effect which the clause would have.

IX. Protecting Confidential Information Through Noncompetition Agreements.

In the high tech era, protection of one’s technology, data, customer lists, and other confidential business information or trade secrets is a sine qua non of success. Departing employees are the biggest risk. Spin-offs or raids by start-up companies or competitors are an everyday occurrence.

The most common way of dealing with this problem is the noncompetition agreement. It is difficult to determine whether someone is violating a nondisclosure agreement, whereas a company can easily find out who is competing with it. Therefore, a comprehensive noncompetition agreement often is the preferred method of protecting against improper use or disclosure of technology.

Noncompetition agreements sweep broadly and that is exactly their danger. They proscribe conduct which society seeks to encourage (competition) and they often extend beyond the legitimate interests of the person or entity seeking protection. The result is that noncompetition agreements are carefully scrutinized by courts. Although flatly prohibited in some states,11 the general rule is that noncompetition agreements are enforceable if reasonably limited in time and geography. It is one thing to put someone out of business temporarily in a particular location; it is something else to leave that person nowhere else to go. Therefore, noncompetition agreements need to be carefully drawn in order to avoid running afoul of statutory and common law restrictions.12

X. Standard Confidentiality Agreement Clauses

Confidentiality agreements usually contain several standard clauses beyond those discussed above, some not unique to such agreements. The utility and desirability of employing such “boilerplate” provisions will depend on the particular situation involved, one’s willingness to rely upon courts to fill in terms not included by the parties, and one’s interest in brevity. The principal standard provisions are discussed below.

A. Nondisclosure and Nonuse

All confidentiality agreements contain a covenant of nondisclosure. Drafters occasionally neglect, however, to include a covenant of nonuse. If the recipient is in a position to use the confidential information in competition with the owner, a covenant of nondisclosure to third parties will achieve only half of the protection desired.

Although in simple agreements the covenants of nondisclosure and nonuse may be combined, in more comprehensive agreements it is often good drafting practice to separate them, inasmuch as the conditions applicable to the covenants may differ. For instance, where the recipient is an individual and is not required to work with others in exploiting the confidential information, the covenant of
nondisclosure usually will be absolute, whereas the covenant of nonuse normally will allow use consistent with the purposes of the particular agreement, such as an employment agreement, consulting agreement, manufacturing agreement, or the like, with an absolute covenant of nonuse arising only after termination of the relationship which gave rise to the disclosure.

B. Acknowledgment of Confidentiality

Most trade secret cases involve as a principal issue the question of whether the information sought to be protected does or does not qualify as a trade secret. An acknowledgment of confidentiality or trade secret status, while not binding on a court or jury, constitutes evidence upon which the owner may rely in asserting its exclusive proprietary rights. It also has the practical advantage that neither the parties who sign confidentiality agreements nor those who pass judgment on disputes find it palatable to assert, or allow to be asserted, the opposite from that which one has previously admitted in writing.

Two further factors influence use of such clauses. First, trade secret cases are usually equity cases, with broad discretion granted to the trial judge. In a close case, acknowledgment of confidentiality may affect the exercise of this discretion. Whether articulated in terms of estoppel or merely general unfairness, the acknowledgment of confidentiality is likely to have some impact on the defendant’s ability to deny that the information sought to be protected is protectable.13

Second, contractual protection of confidential or proprietary information is not strictly limited to information which qualifies as a trade secret. All that is required is that the owner have a legitimate reason (often referred to as a “protectable interest”) for preventing disclosure. An acknowledgment that the information is protectable may influence the determination of the latitude to be accorded to the contractual protection of information which does not qualify as a trade secret.

C. Acknowledgment of Irreparable Harm

In most trade secret cases, the plaintiff seeks an injunction against use or disclosure of the confidential information. Damages are also an available remedy in such cases but often are hard to prove. To obtain an injunction the plaintiff must show irreparable harm. Although irreparable harm often will be presumed in trade secret cases, an owner of confidential information may wish to bolster its position by extracting a prelitigation acknowledgment of irreparable harm and of plaintiff’s entitlement to an injunction. This admission is not binding on the court, but like the acknowledgment of confidentiality discussed above, it may have significant impact, particularly in close cases.

D. Duration

Confidentiality obligations normally are not intended to come to an end with termination of the relationship which occasioned the disclosure of the confidential information: on the contrary, they usually are intended to last as long as the information is confidential. Although one may rely on courts to discern this intention from the particular circumstances, the better practice is to spell out the duration in the agreement.

E. Notification of Subpoena, Compulsory Process

Subpoenas or other compulsory court process often call for production of records which contain trade secrets. These trade secrets are not protected from disclosure unless the owner or the person from whom disclosure is sought makes a special showing, usually by way of a motion for a protective order, that the owner’s interest in secrecy outweighs the need for disclosure in the particular dispute which is the occasion for the subpoena.

The owner will have no opportunity to make such a showing unless it finds out about the subpoena prior to the time the person possessing the records responds. The circumstances of disclosure may or may not create a fiduciary obligation on the part of the recipient either to object to disclosure or to notify the owner of the threat to its rights. Careful owners do not rely on the uncertainties of such implied
obligations; they spell it out in the confidentiality agreements.

A carefully drafted notification clause will cover not only subpoenas and notices to produce but also information submissions or filings required by government agencies. Such information may be available to the general public under the Freedom of Information Act, even if proved to be a highly valuable trade secret.14

F. Ownership of Confidential Information

Disclosures of confidential information rarely contemplate transfer of the underlying ownership rights. These are retained by the owner of the trade secrets. The recipient usually enjoys merely a limited right of use. To make sure that there are no doubts about this point, confidentiality agreements often contain a clause which provides that all ownership rights are retained. Ownership retention may even extend to the documents or media in which the secrets are disclosed such that the owner controls not only the underlying intellectual property rights but also the physical embodiment of such rights whether in the form of a document or a tape or disk. This allows the owner to call in such documents or other media when the relationship which was the occasion for disclosure terminates (see discussion below regarding return of documents)) and reduces the risk of inadvertent disclosure.

G. Return of Documents

When the relationship which was the basis for disclosure of confidential information ends, the owner usually wants all records or other tangible property which contained the confidential information returned or destroyed. A confidentiality agreement should provide for this. Trade secret protection programs normally dictate that trade secrets enjoy the minimum possible circulation. A corollary is that where reuse of or access to trade secret documents is no longer required, the documents should be returned to the owner. One does not want to rely on continued obligations of nonuse or nondisclosure when more practical protection is available through simple physical security measures, such as careful policing of all documents which contain confidential information.

H. Notification of Other Employment

The owner of confidential information wants to be in a position to police the confidentiality obligations owed to it, to be able to anticipate problems, and to take appropriate steps before irreparable damage has occurred. One common situation is the employee, consultant, or other recipient of confidential information who goes to work for a competitor. A solution to this problem is to require notification to the owner prior to commencement of other employment. The following language illustrates such a provision:

In order to allow owner to evaluate risks to its trade secrets and to take steps, if necessary, to protect its exclusive ownership rights recipient agrees to notify owner, prior to accepting any employment (as employee or independent contractor) or commencing any business relating to the subject matter of the Confidential Information.

The owner may even wish to include an outright prohibition of such employment, subject to the limitations applicable to noncompetition agreements.

I. Attorneys’ Fees

Under the law of most states, an owner required to go to court to enforce a confidentiality agreement is not entitled to recover attorneys’ fees unless the agreement says so.15 A confidentiality agreement which does not contain an attorneys’ fees clause therefore may be missing an important term. However, in some states attorneys’ fees clauses are reciprocal, whether drafted that way or not16 and this may be a significant consideration, especially where the confidentiality provision is part of a broader agreement.
J. Choice of Law

Choice-of-law clauses are usually enforceable if the law selected bears some reasonable relationship to the transaction, and subject to the limitation that particular provisions of the law of the selected jurisdiction may not be enforced if contrary to a strong public of the forum jurisdiction.\textsuperscript{17} Confidentiality agreements usually contain a choice of law clause which selects the law of the owner’s home state. Without good reasons or unusually strong negotiating leverage, the recipient is not likely to get the owner to agree to application of the law of the recipient’s state. Consequently, negotiation over choice of law is normally fruitful only if one seeks to obtain the benefit of or avoid a particular law.

If the choice-of-law clause is omitted, the parties are left to the vagaries of common law conflict-of-law rules, with most states now following the “most significant relationship” test rather than the old \textit{lex locus contractus} (law of place of contract) rule.\textsuperscript{18}

K. Venue

Owners who desire to extract the maximum tactical leverage in the event of litigation will include an exclusive venue clause in their confidentiality agreements. This is particularly useful in situations where the confidentiality obligations are included in more comprehensive agreements such as an employment agreement or a joint venture agreement, where there is a risk that the other party will be the one filing suit. In the typical contract case, absent an exclusive venue clause, probabilities are that either party may sue in its own home state. Since litigating long distance is very inconvenient and expensive, being able to avoid having to risk litigation in the other party’s backyard and having the benefit of forcing the other party to incur the expense of coming to your forum constitute a very major advantage.

Footnotes


3. 2 Storey, Equity Jurisprudence 952.


5. Recent cases reflect a split of authority on the issue of protecting nonsecret secrets where the information was acquired in breach of a confidential relationship or through improper means. In Goldberg v. Medtronic, Inc., 686 F.2d 1219 (7th Cir. 1982), the court, applying Minnesota law, held the defendant liable for misappropriation of trade secrets even though the information was public, unbeknownst to the defendant, due to publication in foreign patents. The Minnesota Supreme Court later disapproved the Goldberg holding as constituting an improper statement of Minnesota law. Focusing on the “property rights” rather than the “confidential relationship” theory of trade secrets, applying the newly adopted Uniform Trade Secrets Act (which it treated as merely restating common law principles), the Supreme Court held that one of the prerequisites for a misappropriation of trade secrets claim is that the subject information is, in fact, secret. Breach of confidence alone is not a sufficient grounds for relief. Electro-Craft Corp. v. Controlled Motion, 332 N.W. 2d 890 (Minn. 1983). Compare Kahmin v. Kuhnau, 232 Or. 139, 314 P.2d 912 (1962) (enjoining defendant from using information which, though public, was treated by both parties as being confidential and was communicated to defendant on a confidential basis). See also State Farm Mutual Automobile Ins. Co. v. Dempster, 174 Cal. App. 2d 418, 344 P.2d 821 (1959) (“The contract cannot
make a trade secret out of a situation where none exists.")


7. See 1 R. Milgrim, Milgrim on Trade Secrets § 5.02[4], at 5-40 (1984).

8. See, e.g., Jamesbury Corp. v. Worchester Valve Co., 318 F.Supp 1 (D.Mass 1970), aff’d, 443 F.2d 205 (1st Cir. 1971) (idea reduced to writing after termination of employment held not to be “invention” for purposes of contract, notwithstanding that employee was head of research and developed the idea as part of his job, and left for the specific reason of exploiting it); Regents of Univ. of Colo. V. KDI Precision Prods., Inc., 488 F.2d 261 (10th Cir. 1973) (university hired to invent entitled to retain ownership of invention unrelated to its specific assignment, although contract assignment clause not so limited).


10. See, e.g., Dean Vincent, Inc. v. McDonough, 218 Or. 239 (1978) (suggests that nonnegotiated “boilerplate” liquidated damages clauses are unenforceable).


17. For an example of a court’s refusal to enforce such a clause to a post-employment restrictive covenant, see Frame v. Merrill, Lynch, Pierce, Fenner & Smith, Inc., 20 Cal. App. 3d 668, 97 Cal Rptr. 811 (1971).