SILICON VALLEY LAW GROUP

A LAW CORPORATION

About Terence Church

Terence (Terry) Church is chairperson of Silicon Valley Law Group's Intellectual Property and Technology Licensing group and a member of the firm's Corporate and Securities Group. Terry has served as a senior executive in the legal departments of a number of major technology companies including PeopleSoft, Cisco Systems and LSI Logic Corporation. As VP and Assistance General Counsel at PeopleSoft, Terry's organization was responsible for all inbound technology licensing transactions, strategic alliance engagements, Intellectual Property Management and M&A. He brings a unique combination of legal expertise and business experience resulting in practical solutions to complex problems.

tchurch@svlg.com
tel. 408.573.5700

How to Speed Read an NDA

By Terence N. Church, Esq.

A young acquaintance cornered me at a corporate mixer the other day. He had been invited to a sales presentation for a new product. Upon his arrival, he was handed a non-disclosure agreement (NDA) and told that the meeting was off unless he signed it. The document was two pages of miniscule print. Panicked, he read the document in a fog. Although he signed it, he has absolutely no idea what he signed. He complained that he had no frame of reference with which to review the terms.

In this information age, non-disclosure agreements (a/k/a confidentiality agreements or proprietary information agreements) are as common as bankruptcies in the auto industry. The purpose of an NDA is to restrict further disclosure and use of valuable secret information exchanged between business partners. As with any commercial agreement, potential "gotchas" lurk in the fine print, and careful review is important. It is much easier to evaluate such an agreement – even under pressure – if you have some idea what problems to look for.

The purpose of this piece is to suggest six points to look for and explain how they work.

1. **Definition of "Confidential Information"**. First, locate the definition of "Confidential Information". This answers the question, what information is covered under the Agreement. Often there is a requirement that Confidential Information be marked as such by the discloser (i.e., the party disclosing the information). It's best if the information is delivered in written form, but even if it's delivered orally there is often a condition that Confidential Information be summarized in writing and marked "Confidential". This is best practice for both parties, as it clarifies the parties' obligations.

Some NDAs go on to say that information is covered under the Agreement if it reasonably should be considered to be confidential. This obviously carries a risk of a very unfortunate disconnect between the discloser's expectations and the recipient's

understanding. It is possible to designate certain information or categories of information as confidential regardless of marking, such as the fact that the parties are even talking.

Some agreements say that all information exchanged between the parties in confidential information under the agreement. This is not a good idea for several reasons, not the least important of which is that it is simply not true. It is best to make some effort to define what information is to be considered confidential under the Agreement. As one California court has stated, if everything is confidential then nothing is confidential. If there is no definition of Confidential Information, put one in.

As a practical matter, be sure that whatever designation mechanism is used, it is manageable, i.e., it can be followed. Don't require, for example, that all confidential information is to be printed on pink paper if there are not the resources and management focus to make sure that happens. To be enforceable, the requirements must be clear, and they must be followed.

2. **Scope of Allowable Disclosure**. Corporations can't do anything; it's the human employees that act for the corporation. If the Confidential Information is being disclosed to a company, it will have to be shared among employees of the company. Look for restrictions on this. Often an NDA will say it can only be disclosed to employees who have a genuine need to know for the purpose for which the information is being disclosed.

This is a good practice, especially where the recipient is a large corporation with several divisions or discrete work groups. Look for a restriction against sharing the information beyond a particular division or work group. A related question is whether the NDA allows for disclosure to outside consultants or contractors. If so, check to see if such consultants must have a signed NDA in place with the company to whom the initial disclosure is made.

3. **Standard of Protective Measures**. What measures must the recipient take to prevent disclosure of the Confidential Information? The Agreement should require the recipient to implement at least those protections that it uses to protect its own Confidential Information, but any measures taken should be at least reasonable under the circumstances. In some cases, particular requirements may be set forth, such as access restrictions or network segregation. But look for *reasonable* steps – in most cases that will suffice. If you don't see it, ask to insert it.

4. **Purpose**. This is often missed in an NDA. Restricted disclosure is not the same as restricted use of information. An NDA is also a license because it defines the scope of use that the recipient can make of the Confidential Information delivered under it. Almost always, the purpose of the disclosure is to evaluate a potential business arrangement. Be careful that the NDA does not state the purpose of the deal that's being evaluated. For example, if the parties are discussing a software development deal, there is a temptation to state the purpose of the NDA in terms of the development deal itself. This can lead to an unintended license for the recipient to use the Confidential

Information to develop the software. Not good. The terms of that license should be addressed in a later agreement that supersedes the NDA.

5. **Term of the Agreement**. In an NDA, there are two time periods at play. One is how long the agreement itself is in effect. This is what is normally thought of as the "term" of the agreement and defines the period during which the disclosure of the Confidential Information creates obligations for the other party to protect it. It might be six months or several years, and it runs from the moment the NDA is signed. The terms and obligations imposed in the NDA do not apply to confidential information disclosed after its end date.

The other period of time is how long the obligation to protect the Confidential Information continues to exist. This is normally beyond the term of the agreement – i.e., it survives the end date of the NDA -- and depends on the anticipated "shelf life" of the information, or how long it is likely to hold its unique value for the discloser. This period of time is often three to five years and commences to run either when the Confidential Information is disclosed or is measured from the termination of the NDA. Look for both of these time periods in the NDA.

6. **Right to Return of the Confidential Information**. Most NDAs require that when it terminates, the recipient must return the Confidential Information to the discloser. In today's world of networks and back-ups, it is virtually impossible to return all copies of the Confidential Information. The NDA should include a provision that the discloser may require the recipient to certify the destruction of the Confidential Information and all copies of it. It should also require destruction of all analyses, tests, benchmark studies and derivative works and any other documents from which the Confidential Information can be viewed, used or extracted.

NDAs are common in modern hi-tech commerce. But don't confuse common with benign. NDAs are essential to protection of valuable trade secrets. Use them, sign them and honor them. But read them first. If you see these six points addressed in an NDA you are presented with, you have a better chance of being protected and of protecting your valuable information.