On the Drafting of Confidentiality Agreements

Drewsen, Merete; Lando, Henrik; Cummins, Tim

On the Drafting of Confidentiality Agreements

Merete Drewsen, Henrik Lando and Tim Cummins

Abstract

This is not a theoretical paper but an application of existing law and economic contract theory to the issue of how to draft a specific kind of contract. It is addressed to practitioners and is intended for practical use. It will be part of a Wiki (as in Wikipedia) for contract drafting, which IACCM (International Association for Contract and Commercial Management) has initiated. The main theoretical aspect of the article concerns the application of the value maximization principle (the Coase theorem) to the drafting of confidentiality agreements. While the article is not theoretical, its prescriptions are open to theoretical dispute; this may especially be the case for the section on the size of damages.

Introduction

The considerations fall in two parts. The first part provides a general economic principle for the drafting of confidentiality agreements. The second part applies the principle to more specific considerations concerning the scope, duration and damages for breach of confidentiality agreements.

1. The general principle of value maximization

As a negotiator of confidentiality agreements, your challenge is to find the agreement, which creates the greatest total value. This principle of value-maximization suggests a win-win attitude towards negotiations and also provides a principle for drafting specific terms. An example can illustrate why it is rational to seek value-maximization rather than terms that are in your interest only: Consider the situation where you must hand over sensitive information to the other party and where the issue is the degree to which the other party should protect that information. The recipient may e.g. want to be able to circulate the information among employees, because doing so will allow the employees to make decisions on their own, but circulation may create a risk that an employee will leak the information to a third party (perhaps upon leaving the firm). In this situation, the value maximization principle provides a simple rule: If the loss to the recipient from not being allowed to circulate the information is (approximately) 10, and if the value to you of avoiding the risk of a leak is (approximately) 20, circulation should be disallowed, since this creates a surplus of 20 - 10 =10, that can be shared between you. You might pay the recipient 15 up front for committing not to circulate, or the price of the underlying contract price can be adjusted, and you both gain 5. On the other hand, if the loss to the recipient of not being permitted to circulate is 30, the loss is 10 from banning circulation. The example illustrates that it is rational to follow the principle of agreeing to such terms that create maximum value overall, i.e. such terms for which the difference between benefits and costs (in monetary equivalents) is maximized.
Another way of stating the principle is in terms of marginal benefits and costs: For example, when the issue is the degree of precaution taken by the recipient in lowering the risk of dissemination to third parties, precautions should be taken up to the point where the marginal benefit (the value to

the owner of the information) of extra precautions outweighs the cost to the recipient of taking these extra precautions. You should seek that balance between (marginal) benefits and costs.

The principle of value-maximization stands in contrast to the strategy of taking advantage of a superior bargaining position. The idea is that also when you are the stronger party, able to impose your terms, you do better in seeking efficient, value-maximizing (and hence reasonable) terms, instead of using your bargaining strength to obtain a one-sided agreement. Not because value-maximizing terms tend to be fair and reasonable (though that is a benefit), but because the superior bargaining position is better employed in extracting a favorable price than in imposing one-sided contract terms that destroy value.
In practice it is of course challenging to find the value-maximizing agreement. First, benefits and costs may be difficult to estimate and, second, may be known only to one party. On the first point, costs and benefits have to be estimated as best possible; errors are bound to occur, but the point is that more errors will be made if no attempt is made to quantify the importance of contract terms. The second point is more fundamental; it may not be in your interest to reveal your costs and benefits, and this may be an obstacle to finding mutually beneficial terms. However, in many circumstances, this barrier can be overcome, especially if some measure of trust can be generated in the relationship. Even when trust is limited, it is worth keeping in mind the value maximizing agreement as an ideal benchmark, often you can gain more by expressing your concerns and your aims (without divulging everything) than to keep silent, because the value that can be gained through creative problem solving tends to be significant. The principle of value-maximization guides specific considerations concerning mainly the scope and formulation of protection, the duration and the remedies of the agreement.

2. Specific Considerations

2.1 Scope

Prior to the decision which kind of information to include in a confidentiality agreement is the decision which kind of information to exchange in the relationship. Are there particular types of information that either you want to receive or specifically do not want to receive? Can these be defined, placing limits on the scope of the confidentiality agreement? A typical exception might be information that is owned by a third party, whether or not that party is involved directly in this relationship. It is worth considering carefully,which information to exchange, since if the information is exchanged and also included in the confidentiality agreement, the obligations created by confidentiality provisions can be onerous and costly to administer.
At this stage, you may also consider whether the information received should be handled as a matter of course (e.g. according to the company’s regular quality manuals) or whether you want such transfers to be highlighted and agreed on a case by case basis.
When having decided on which kind of information to exchange, the next decision is which of this information to protect in the confidentiality agreement. Treating all information as confidential may well be costly, and a balance must be found between the benefits and the costs of confidentiality. The need for considering the proper scope of confidentiality arises e.g. when the initiating party seeks a broad definition (see examples) that maximizes their coverage and the other side's obligations. Or when one party seeks to make the clause unilateral (i.e. applying only to their own information). As a negotiator, you must decide which scope of the clause is value-maximizing (which will at the same time tend to be also a `reasonable´ scope) and whether it should be mutual.

An example of the balancing between costs and benefits arises when one party (usually the customer) seeks to restrict the way that the other party deploys personnel who have been involved with the contract and its fulfillment. For example, development or implementation teams may acquire sensitive information or know-how that would assist a competitor. The negotiator must address these valid concerns; this involves a need to understand the real scope of the other party's fears. Clearly, a blanket provision that prevents future deployment of staff is not acceptable, but some constraints on where they work or the types of projects they work on, for a specified period, may represent an acceptable compromise.
As another example of the cost-benefit approach, as a negotiator you should understand the standard policies and procedures of your Principal and seek terms that are consistent with standard capabilities in safeguarding confidential information. Otherwise compliance will become too costly.

In some cases, it is clearly worth restricting the scope of confidentiality by excluding some kinds of information from the agreement. Two important examples stand out:
1. The recipient may need to reveal the information to a third party. For example, the second party may be a researcher who is motivated by the prospect of publishing. Or, it may be that the other party must subcontract for a component that requires the subcontractor to understand the workings of a machine. The second party cannot then be bound by a confidentiality clause not to reveal the workings of the machine to the sub-contractor. Care must then be drawn to prevent the subcontractor from revealing the information to others, and to prevent the subcontractor from benefiting from the information in other ways than intended. But clearly the disclosure of the information to the sub-contractor should be explicitly excluded in the agreement between you and the other party.
2. The information may already be available to third parties (already´ in the public domain´) or it may be likely in the near future to fall into the public domain from other sources. Protecting such information makes little sense and may cast doubt on the protection in the agreement of other information that it does make sense to protect. Special provision is also worthwhile for information already in your possession as when the information has already been developed in your research laboratory.
There is also the practical choice whether confidentiality terms should be contained in a stand-alone agreement (such as a Nondisclosure Agreement) in which case they operate in isolation from any other contractual arrangement or discussion. Or to include them as terms within a broader agreement, in which case the terms have natural links to other clauses that must be considered by the negotiator. These may include Purpose, Limitation of Liability, Non-compete, Publicity, Continuing Obligations, Term and Termination and Indemnities.

2.2. The Formulation

Several issues arise when it comes to the way in which the information is included or excluded in the agreement.

You must consider:

-whether to use vague or specific terms in describing the information to be included or excluded. A specific term is especially warranted when it is clear to one but perhaps not to the other or to a third party adjudicator that a given piece of information is, or is not, worth the cost of confidentiality. Then a vague term may not be interpreted correctly, and writing a specific clause concerning this piece of information will then be worthwhile when the drafting costs are not too high in comparison

with the value at stake. A specific term provides better incentives to avoid breach of the particular kind of information, aligns expectations better and prevents disagreement whether breach has occurred or not. Another advantage of specific terms is that written information, e.g. concerning methods and know-how, which is provided specifically for the term of the agreement, may be accompanied by specific obligations for all copies to be returned or destroyed on termination. These benefits must be weighed against the drafting costs.

-whether to specify the information which is included or to specify the information excluded. When the included information is specified, it may be stated that all other information is not included, and when the excluded information is specified, it may be stated that the residual is included. Naturally, you can also explicitly include some kinds of information and specifically exclude other kinds, and you may then leave the residual either protected, unprotected or protected according to a general term (stating that the recipient is under a general obligation not to reveal sensitive information).

-whether to specify the sources through which confidential information must pass. For the recipient, it is clearly easier to build a management system if qualifying information is marked and / or if it comes only from or to specified individuals or departments. The parties may wish to have even tighter control of the confidential information, designating that only specified individuals will have access to the confidential information, in which case the names, titles and contact information for those individuals will be identified in the confidentiality agreement. Another means of controlling the dissemination of the confidential information may be that one of the parties or both may wish that only those people who have a need-to-know status related to the project will be given access the the confidential information. In this case a general statement is placed in the confidentiality agreement. Then only an audit of the situation may reveal compliance or lack of compliance.
-whether to build a system that eliminates doubt concerning the exchange of information. One system used is for the recipient of the confidential information to provide acknowledgement of the receipt of information by a written document with a synopsis of the confidential information received, and conveyed to the owner of the confidential information within a certain period of time. Although avoiding doubt, this approach often will be reluctantly accepted as it requires time and administrative effort for compliance.
.

2.3. Duration

The benefits for the first party of secrecy is likely to fall over time (although it may well outlast the length of the contract with the second party in which case protection should be extended beyond he duration of the contract), whereas the cost of compliance to the second party, e.g. the monitoring of employees, may not fall over time to the same extent. At one point, the benefits are likely to become smaller than the costs (including potential dispute resolution costs), and it is therefore generally optimal to limit duration. In principle, for any given piece of information, confidentiality should extend until that point in time where extending it further generates more costs than benefits. Obligations may have several conditions that relate to their potential duration.
1. A specific term, which may either start with the receipt of the information (which must then be recorded), or may be a period following termination of the agreement or contract (a 'continuing obligation');
2. A dependency on external events - for example, if the information enters the public domain by means other than breach,
3. Specific notification or authorization by the owning party.

2.4. Sanctions for breach

Sanctions should be set mainly with a view to ensuring that the recipient has an incentive to live up to the agreement. They should be set such that incentives to avoid dissemination are neither too great (leading to too much caution) nor too small (leading to irresponsible handling of information, or perhaps to intentional disclosure to third parties).

Penalty for breach takes three forms:

-A loss of reputation and if breach leads to termination (not always the case), loss of the future profits from cooperation

-Conscience costs: The breaching party may feel guilt or bad conscience for having breached a contract; this may be viewed as a self-imposed sanction that increases the overall sanction from breach. This kind of sanction may well be important and in some situations even sufficient to induce correct behavior; this is the case where trust render other kinds of sanctions unneccessary.

-Damages

As a general principle, the sum of the three kinds of sanctions should be so high as to deter the second party from intentionally revealing the exclusive information, and as to induce the party to take due care to prevent unintentional dissemination. This means that the expected sanction, i.e. the size of the sanction multiplied by the probability that it will be applied, should equal the (monetary equivalent) of the loss to the first party from the breach. To exemplify, if breach is discovered only one in ten times it occurs, the total sanction (including the monetary equivalent of the reputation and conscience costs) should in principle be ten times the size of the loss (abstracting from the fact that especially in common law, liquidated damages that exceed the loss may not be upheld in court). The point is that incentives to avoid dissemination are correct, i.e. total value-maximizing, when expected damages equals the loss. Thus, if the expected sanction is higher than the loss, it can be demonstrated that there will be excessive care, i.e. the breaching party will do too much to avoid dissemination, and will feel too constrained in the handling of information- more constrained, that is, than is justified by the loss from breach to the first party. On the other hand, if the expected sanction is lower than the monetary equivalent of the loss to the first party, the second party will find it uneconomical to take precautions that are in fact justified by the loss to the first party of the information being disseminated. In other words, the principle of equating the expected sanction with the loss is value maximizing. It should be stressed that both parties gain from setting sanctions at the value-maximizing level: a greater pie can be shared in a way to make both parties better off than they could be with a smaller pie.
Some conclusions will now be drawn from the general principle in terms of how sanctions should be set under varying circumstances. In particular, it will be addressed
1. how the existence of conflict resolution costs affect the optimal sanction
2. how the optimal sanction depends on the probability that breach will be discovered and on the size of the reputation loss to the breaching party.

Ad 1. Breach, if discovered, may be accompanied by legal costs, either to reach a settlement or to conduct a trial; such costs may well be significant. These costs should be added to the cost of

breach both to the breaching party and to the party whose information is disseminated. Such legal costs hence act as deterrence for the breaching party, but at the same time increase the total cost of a breach to the aggrieved party. Overall, such costs render it more important to avoid breach (for breach becomes more costly), and this may call for a higher monetary sanction to the extent that if the sanction becomes high enough, it may prevent breach and hence also prevent the legal costs associated with breach. However, if the loss from breach is relatively small, the opposite solution can be appropriate, namely to exclude liability for dissemination of the kind of information in question. Sometimes the cure of a legal dispute may be worse than the disease of breach of confidentiality. Such instances are more likely when the breach is unintentional, perhaps beyond the direct control of the liable (legal) person.

Ad 2. If there is a significant probability that breach will be discovered, and if the breaching party loses important reputation capital when it occurs, there is less need for monetary damages. Under certain circumstances, reputation may in itself provide an adequate incentive for the second party to avoid breach, and there is then little reason to involve the legal system, i.e. to rely on high damages. On the other hand, the prospect of a court verdict (or a disclosed settlement) may further the reputation incentive, for without a verdict or a settlement, it may not be possible for third parties to know whether a breach has in fact occurred. The two kinds of sanctions then complement each other, and it is important that the first party can be expected to pursue the matter legally; it may then be important to set liquidated damages such that the first party will be incited to bring a claim against the breaching party, i.e. to ensure that a law suit will have a positive net present value to the claimant.

Frequently, breach will become known to important market players also in the absence of a legal verdict. When that is the case, the following principles for setting liquidated damages apply.

	High reputation loss	Low reputation loss
High probability that breach is discovered	Little reason to stipulate high monetary sanctions unless loss from breach is very significant	Damages should be set near the size of the loss from breach (or one can rely on the legal default rule)
Low probability that breach is discovered	Monetary damages may be necessary because the low probability of detection requires a very high sanction for there to be deterrence	High liquidated damages are necessary, potentially several times higher than the actual loss

When, on the other hand, a court verdict is a condition for third parties to know whether a breach has in fact occurred, the table should be changed in one respect. The parties should then stipulate significant liquidated damages also when the probability of discovery of breach is high and when reputation is important. Unless damages are high, the threat to litigate in the event of breach may not be credible, weakening the reputation incentive to avoid breach.

In principle, different sanctions should apply for different kinds of information, but often this degree of detail is excessive in terms of drafting costs. One possibility is then to set liquidated damages that apply to dissemination of any kind of information and to preserve the right to claim damages equal to the loss if the loss is higher than the liquidated damages. This solution offers the advantages that the liquidated damages alert the second party to the importance of the matter, and the right to go for further damages offers some protection against very important breaches. But note that this solution does not address the problem of the low probability of detection.

2.5. Some other specific issues

2.5.1. The standard of liability and the liability of third parties

A negotiator must consider the liability rule, i.e. whether it is only required that reasonable steps are taken to protect the data (a negligence rule), or whether the recipient firm becomes liable whenever information is leaked from the firm (strict liability).
This issue of the liability rule (whether negligence or strict liability) often arises when the recipient of information must bind employees or a subcontractor through a secrecy clause or a confidentiality agreement. One of the purposes of the confidentiality agreement is exactly to induce care in drafting the secrecy clause. In this context, the first issue which arises (as noted in `Drafting International Contracts, an analysis of contract clauses´ by Marcel Fontaine and Filip De Ly, Transnational Publishers, Inc, 2006) is who the third party is liable to. It is worth specifying that the third party is liable to the second party for the breach and that the second party is liable for breach of the third party. The question then arises whether the second party should be strictly liable or only liable if the second party did not take adequate measures to prevent the third party from breaching. The answer hinges on whether the measures are observable or known only to the party undertaking them. For example, the effort exercised in instructing employees about the importance of maintaining confidentiality is not observable and hence it will not be possible for the first party to prove that the second party took too little effort. Then it may be better to hold the second party liable whenever the third party disseminates the information, i.e. on the basis of strict liability. If the most important measures are observable, on the other hand, the rule of negligence might be preferable.

2.5.2 The burden of proof

The issue arises who should prove that the information has in fact been disseminated by the recipient, when it is found in the possession of a third party. The second party may have to prove that he or she has not disseminated it, or the first party may have to prove that the second party has done so. The standard of proof is preponderance of the evidence and there may be a preponderance of evidence irrespective of who has the burden to prove it. But in general the burden of proof should from an incentive viewpoint lie with the party who can produce evidence more easily, or, if it is likely that neither of the party can produce the evidence, it should lie with the second party if this strengthens the incentive to take (unobservable) precautions.

Note that if the burden of proof lies with the second party it may be harder to convince the second party to accept a high sanction. If the parties agree on strict liability or on reversing the burden of proof, the sanction should be lower.

References

Marcel Fontaine and Filip De Ly, *`Drafting International Contracts, an analysis of contract clauses´* Transnational Publishers, Inc, 2006

Edmund W. Kitch, *´The Law and Economics of Rights in Valuable Information'* **,** *Journal of Legal Studies*, Vol. 9, No. 4, The Law and Economics of Privacy (Dec., 1980) , pp. 683-723