Confidentiality and non-disclosure agreements

22 JUN 2012
By: Andrew Lord | Ted Maduri

Many inventors and businesses spend considerable time and resources developing new products or building customer bases. It is not surprising, and certainly justified, to see great care taken to ensure such proprietary information does not fall into the wrong hands. However, to take a promising idea, or business, to the next level, a business typically needs to share its valuable secrets with prospective strategic partners or investors. Signing an effective non-disclosure agreement (“NDA”) can therefore be a critical step in developing a new business relationship or opportunity by giving the parties enough comfort to take that initial step.

This article discusses: 1) when NDAs are appropriate, 2) what type of information should be covered, 3) what type of information should not be covered, 4) typical protective measures, and 5) how to address breaches and the ultimate termination/survival of an NDA.

1. When is an NDA appropriate?

As part of just about any commercial arrangement or corporate transaction, parties should ensure that they agree to confidentiality provisions that are sufficiently protective, that accommodate the practicalities of getting the deal done, and that will survive to an appropriate degree if the arrangement or deal either closes or falls apart. NDAs should obviously be in place for M&A transactions and licensing arrangements, but they should also be considered in various other relationships like consulting services, advisory board engagements and outsourcing arrangements. When parties are just beginning to discuss a potential arrangement or deal, an NDA may or may not be appropriate. The parties may still be holding their cards closely at this stage and not exchanging significant confidential information. As the parties dive deeper into due diligence and negotiations, the exchange of confidential information will intensify and outside advisors may become more heavily involved in analyzing the deal. Ideally parties should put a formal NDA in place prior to sensitive information being exchanged. The scope of an NDA depends on the type of information that is being disclosed, the purposes for which it is being disclosed, and the need for such information to remain confidential in the long term.

2. What type of information should be covered by an NDA?

While it may seem obvious to say, confidential information can only include information that is already confidential. In determining what type of information can properly be characterized as confidential, consider the following list of factors identified in Pharand Ski Corp. v. Alberta:

- the extent to which the information is known outside the party’s business;
- the extent to which it is known by employees and others involved in the party’s business;
- the extent of measures taken by the party to guard the secrecy of the information;
- the value of the information to the party and its competitors;
- the amount of money or effort expended by the party in developing the information; and
the ease or difficulty with which the information could be properly acquired or duplicated by others through their independent effort.

Considered collectively, these factors can assist in determining whether information is confidential and the degree to which a party should attempt to protect it under an NDA.

Not all valuable information is confidential. For example, an employee’s skills and general knowledge may be enhanced by having worked for a particular employer, but such trade knowledge is not necessarily confidential information of that employer. Consultants who are not employees often want to be free to make further use of skills and general knowledge they acquire during an engagement and therefore often seek to include a “residual knowledge” carve-out in NDAs.

Given that there is some uncertainty in the definition of confidential information at large, parties should take care in defining “confidential information” in an NDA. Confidential information may be defined to include information

- exchanged prior to the execution of the NDA (or other agreement containing confidentiality terms);
- exchanged orally, in writing or in any other form or medium (e.g., by email);
- observed by a party (e.g., on a site visit);
- that is marked confidential or not;
- that a party ought reasonably expect to be confidential;
- that is derived from confidential information;
- that pertains to the existence or terms of the negotiation between the parties; or
- received from or regarding subsidiaries or third parties.

Disclosing and receiving parties will often have different perspectives on the appropriate scope of confidential information. A disclosing party will likely prefer a broad definition and should resist the need to mark or otherwise identify information as being confidential. A receiving party will likely prefer a narrower definition as to what would constitute confidential information (and would typically prefer clear marking of same). This may be particularly true where there is a potential for the disclosing party to provide more information than is needed, leaving the receiving party more broadly constrained by the NDA than is reasonable or necessary. If personal information will be disclosed, the NDA should include specific privacy provisions to comply with applicable privacy legislation.

3. What type of information should not be confidential?

Not all confidential information should be treated as confidential. There are two ways to exclude categories of possible confidential information: 1) by including exceptions to the definition of confidential information or 2) by adding carve-outs to the obligations that apply to confidential information. The second approach is generally more straightforward but the following should be excluded one way or the other:

- Information developed by the receiving party prior to disclosure under the NDA (without reference to the confidential information);
- Information received by the receiving party lawfully from third parties (without breach of confidentiality obligations);
- Information derived independently by the receiving party (without reference to the confidential information) after disclosure under the NDA;
- Information already in the public domain, including information disclosed in court or regulatory proceedings, through no wrongful act or omission of the receiving party; and
- Disclosure compelled by law or court order.

Where disclosure is compelled by law or order, an NDA cannot contradict this legal obligation. As a result, NDAs should not have disclosure language such as “under any circumstances” or “for any reason,” otherwise the entire agreement may be in jeopardy. That said, an NDA should impose a duty on the receiving party to notify the disclosing party of the request for disclosure, if permitted. The receiving party should only be permitted to disclose such information to the extent specifically required under the applicable law or order. The receiving party should also be required to use commercially reasonable efforts to oppose such requests for disclosure where there are reasonable grounds for doing so, and to seek protection or continued confidential treatment of the information.

In addition, special care should be taken when entering into NDAs with public authorities who may be subject to
freedom of information requests. Such NDAs should ensure that the disclosing party is given reasonable opportunity available under the applicable freedom of information legislation to oppose the disclosure of its confidential information. Disclosing parties should understand in advance what types of information is or is not confidential for the purposes of freedom of information requests. For example, commercial terms negotiated with a public body may be viewed by the private party as extremely sensitive competitive information but may nevertheless be subject to disclosure in response to a freedom of information request.

4. What level of protection should apply to confidential information?

It is not unusual to see very detailed definitions of confidential information and then a very basic use/disclosure provision, which almost defeats the purpose of having put an NDA in place. One of the most important features of an NDA is a specific description of the purposes for which confidential may be used, paired with a blanket prohibition on using it for anything other than the prescribed purpose, so as to prevent the receiving party from making inappropriate use of valuable confidential information. Typical uses of confidential information may include: carrying out specified professional services (e.g., engineering, software needs assessment, management consulting engagement); conducting due diligence on an acquisition target company; exploring the terms of a potential joint venture or other business opportunity; etc.

Parties should consider the level of care that must be taken to avoid disclosing confidential information. It is not unusual for a receiving party to propose that it will use the same measures to protect a disclosing party’s information as it uses to protect its own confidential information. This type of subjective standard is often insufficient. Disclosing parties should instead insist on a more objective standard, such as the use by the receiving party of commercially reasonably efforts to protect the information of the type being disclosed.

A disclosing party may want to include specific protective measures such as:

- a requirement that information be kept in a secure location and not removed therefrom without prior written consent of the disclosing party;
- specific security protocols for data systems where confidential information will be stored;
- limits on access to information, including limitations on disclosing information to employees or professional advisors;
- notification of unauthorized disclosure/misappropriation;
- limits on copying information or transmitting it electronically; and
- restrictions on destroying confidential information without prior written consent of the disclosing party.

Care should also be taken in defining who can receive confidential information in furtherance of the permitted or specified purpose. Often, there is a reasonable need to disclose information to employees or professional advisors (or even financing sources, affiliates or limited partners, etc.) but this should be considered on a case-by-case basis. Ideally, such recipients are identified by name, but at least should be identified by class, and always on a “need to know” basis. The parties should be clear about what confidentiality obligations must be imposed on such third parties as a prerequisite to them receiving confidential information. Employees may be subject to confidentiality obligations as part of their employment agreements. There are a few ways to handle disclosure to professional advisors: a) they could be asked to become a party to an NDA, b) they may just have to agree to keep information confidential, or c) the parties may simply rely on obligations of confidentiality imposed on them by their professional governing body. Disclosing parties should seek to have the receiving party accept liability for confidentiality breaches by employees, advisors, affiliates and other necessary recipients, although this request may be strongly resisted by the receiving party.

It never hurts to be explicit in an NDA that information should never be disclosed to a party that competes with the disclosing party. This may be a particularly contentious issue where, for example, a potential buyer of a disclosing party also has (or could have in the future) interests in competitors of the target. Where a party has a number of affiliates, some of whom may compete with the disclosing party, significant time can be spent negotiating whether the NDA should apply to affiliates, which parties generally resist, or whether it should prohibit disclosure to affiliates, which may be difficult in practice if, for example, individuals involved with the receiving party are also involved with the affiliates (e.g., as board members or shareholders).
5. What happens in the event of termination or a breach?

Parties should also consider how long information should remain confidential. Every disclosing party would prefer to have their information held confidential forever. More typically, confidentiality provisions in commercial transactions survive for around two years. Any personal information should be held in confidence indefinitely. Again, the appropriate sunset for confidentiality obligations will depend on the nature of the information. Parties should include a reasonable sunset, failing which a court may impose one on them.

Every NDA should specify the parties’ obligations upon termination of the NDA. Usually, there will be an obligation to return confidential information, sometimes only upon receipt of written request, or to certify that all copies of same have been destroyed, sometimes in accordance with specific protocols (e.g., for truly deleting information from hard discs). However, there is typically some real discussion about whether these obligations should be subject to carve-outs that allow the receiving party to retain copies to the extent required by law (e.g., for income tax purposes or in compliance with accounting standards) or as required in accordance with internal record-keeping requirements. They may also address the practical difficulties of deleting data from electronic databases which may be routinely archived for disaster recovery purposes. Such carve-outs should carefully describe the circumstances under which such retained information can be accessed/used after termination. If a receiving party cannot justify a reasonable purpose for retaining the information, the carve-out may not be appropriate.

From the receiving party’s perspective, well-drafted NDAs should: a) address the consequences of a breach of confidentiality, which may vary depending on whether the breach was intentional, negligent or without fault of the party in breach; b) expressly preserve the right of the disclosing party to seek equitable remedies by acknowledging that a breach can cause irreparable harm that cannot adequately be compensated with damages; and c) include indemnification for any loss or damage (including third party claims) arising from the breach.

Summary of Tips

- Disclosing parties should broaden the definition of confidential information and should resist requirements to identify information as confidential; receiving parties should do the opposite; in either case, care should be taken in defining confidential information.
- Unless the parties intend otherwise, make clear that information disclosed by a party, and all intellectual property rights thereto, should remain the property of the disclosing party.
- If confidential information will include personal information, include privacy covenants and ensure that the NDA survives indefinitely with respect to personal information.
- Carve-out the typical exceptions for the treatment of otherwise confidential information;
- If the NDA includes a carve-out of confidential information compelled by court or other order, include requirements regarding notice to the disclosing party, limitations on the scope of disclosure, efforts to oppose disclosure, and efforts to seek confidentiality protection for information that must be disclosed.
- Understand the impact that a freedom of information request may have on information that the parties have agreed is confidential.
- Precisely describe how confidential information may be used and prohibit all other uses.
- Include an objective standard for the level of care that a receiving party must use in protecting confidential information; add all desired protective measures.
- Understand what types of employees, advisors, affiliates and other people will need to receive confidential information and ensure that each such recipient is subject to appropriate confidentiality obligations.
- Choose a survival period that makes sense in the circumstances (two years is typical).
- Include clear obligations in the event of termination and take care in defining any rights that parties have to retain confidential information after termination to comply with, for example, record-keeping or retention policies.
- A potential acquirer of a disclosing party should not be permitted to solicit employees of the disclosing party if the deal does not proceed, subject to some carve-outs (e.g., permit general solicitations for employment).
- Where the parties are in different legal jurisdictions, the NDA should address choice of law and of forum. This may be the first time this possibly contentious issue arises between parties from different jurisdictions.

AUTHORS

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com. This may qualify as
Andrew Lord
Partner
Toronto | T: +1 416 365 3500
[email protected]

Ted Maduri
Partner
Toronto | T: +1 416 365 3500
[email protected]