Tips for Working Under an NDA

By Stephen Murray

Occasions may arise where parties collaborate on a project involving proprietary or otherwise sensitive information. To prevent that information from being misused, shared, and/or publicized, the parties often enter into a non-disclosure agreement (NDA). However, breaching an NDA can have serious consequences, even in cases of accidental misuse or disclosure. Below are some basic steps you can take to protect yourself and your company if you are working within the confines of an NDA.

Ask to See and Review the NDA

Executives or counsel typically negotiate NDAs, but the terms most directly apply to the engineers or others working with the received confidential information. Nonetheless, those engineers often never actually see the agreement. If you anticipate receiving or using confidential information, ask to review a copy of the NDA. This practice can substantially reduce the possibility of inadvertent disclosure or accidental misuse of the information – it is easier to comply with obligations when you know what they are. Significant provisions to review include the definition of confidential information, the duties attached to receiving that information, and the length of time those duties will last. If there is something in the agreement you do not understand, ask for an explanation. This may come from an attorney for the company or someone involved in negotiating the agreement that hopefully better explains the contract's terms. For your own sake, be fully informed of your responsibilities for handling someone else's confidential information.

Set Automatic Calendar Reminders

NDAs often include multiple dates. For example, although an NDA's basic terms could expire tomorrow, the parties may still have to avoid disclosing or using confidential information for another two years (or more). An NDA can also have a deadline for returning or destroying confidential information in the receiving party's possession (e.g., ten days after expiration). Setting automated reminders can prevent you from overlooking actions that need to be performed. Many agreements expire well after work has ended, so some actions might otherwise slip through the cracks because the NDA is no longer front of mind. For example, forgetting to return confidential material to the disclosing party can create adverse inferences in a potential dispute, either by implying that you used the information still in your possession or by providing an opportunity to mistakenly use it contrary to the agreement. An automated reminder can help you remember that the confidential information you used six months ago needs to go back to its owner or be destroyed. Of course, many companies have an attorney or some other designated individual collect that information when the time comes. Still, it does not hurt to protect yourself in case your company does not have the resources or they forget you had relevant information.

Keep Relevant Information Centralized and Safe

Accidental disclosure or misuse is more likely to occur when access to confidential material is unfettered, such as when documents are lying precariously on a desk. Suppose you are responsible for handling confidential information. In that case, physical embodiments, e.g., printed documents, prototypes, samples, etc., should be kept in a single, preferably securable location, such as a lockable cabinet. If others require access to the information in your care, it may also be advisable to have them sign in and out when removing and returning the materials. That way, it can be easier to track who has what and where.

Digital information is trickier, but comparable procedures can be implemented. Many companies (particularly after Covid accelerated the transformation to remote work) now have centralized servers or cloud-based document storage options. If the disclosing party allows, it is preferable to set up a folder or other similar structure in the server or cloud and store (and have others store) documents referencing or relating to the confidential information in that location, rather than on your local hard drive. This reduces unnecessary and uncontrolled proliferation, but appropriate security safeguards should be implemented to prevent unauthorized outside access. Password protection of the folder or other types of restrictions should also be put in place to prevent access by particular internal users. Many document management software programs can limit folder access to select individuals or groups and wall off others. In some programs, the very existence of the file or folder may be invisible to those without proper credentials. It is much easier to maintain control over confidential information when it resides in one or two known and secured locations, as opposed to being scattered between offices or individual personal computers.

If You are Confused – Ask for Help

Many NDAs require that confidential information be marked as such – for example, by placing a "Confidential" or similar label on appropriate documents. This allows you to clearly distinguish between information that needs protection and information that does not. But NDAs are usually very forgiving when the disclosing party either forgets to label or over-designates. It is in your own best interest to make sure a disclosing party follows the rules. If information is received that may only arguably be confidential and is not marked, or if non-confidential information appears to be improperly designated, bring it to the disclosing party's attention and get the issue resolved right away. Avoid a dispute that a jury must decide and make the disclosing party be clear upfront. ▪

*Stephen Murray is a Partner at the intellectual property firm of Panitch Schwarze Belisario & Nadel. He focuses on protecting intellectual property, particularly patents, for clients of all sizes ranging from individuals to multi-national corporations (**smurray@panitchlaw.com**).*