Intellectual Property & Technology Law Journal

Edited by the Technology and Proprietary Rights Group of Weil, Gotshal & Manges LLP

VOLUME 34 • NUMBER 7 • JULY–AUGUST 2022

Top Tips to Protect a Company's Confidential Information When Sharing with Others

By Jason W. Balich and Brandon S. Blackwell

A company's confidential information, trade secrets, and know-how – key components of its intellectual property[1] – are often what sets it apart from competitors. Yet to grow and thrive, companies routinely need to share their information with outsiders: contractors, vendors, consultants, distributors, and even prospective customers. How then does one both collaborate with others and protect confidential information?

It is all too easy for a company to lose control of its intellectual property in just a few missteps. Take Tax Track, a Minnesota company that developed a new spin on leveraged life insurance and started pitching the idea to others. In some cases, Tax Track got the people it pitched to sign a nondisclosure agreement ("NDA"), including New Investor World. But Tax Track also pitched the idea to others without an NDA in place. When New Investor World brought a competing product to market, Tax Track sued for misappropriation of its confidential information. But the courts refused to enforce the New Investor World NDA – Tax Track's disclosures to others in the absence of an NDA made the innovation part of the public domain and no longer protectable.[2] Tax Track dissolved that same year.

Collaboration with others and protecting proprietary information do not have to be mutually exclusive. Both are achievable through consistent use of a few practical measures of protection.

PUT A PLAN IN PLACE TO PROTECT CONFIDENTIAL INFORMATION

Best practices for exchanging confidential information start with establishing a plan and consistently following it. The plan should cover what information will be sent to and accepted from outside parties, how that information will be used both internally and by the outside party and what measures will be used to protect the information.

DEFINE WHAT INFORMATION WILL BE SENT OR ACCEPTED

Even with an NDA in place (discussed more below), it is important to first consider what confidential information should be shared with outside parties and what confidential information should be accepted from them.

Take trade secrets, for example. While trade secret law varies among jurisdictions, it usually requires that "reasonable measures" are employed to protect the trade secret. Having an NDA is not always

Jason W. Balich is a litigation associate at Wolf, Greenfield & Sacks, P. C. **Brandon S. Blackwell, Ph.D.**, is a shareholder in the firm's Chemical & Materials Technologies and Mechanical Technologies Practice Groups. Resident in the firm's Boston office, the authors may be contacted at jason.balich@wolfgreenfield.com and brandon.blackwell@wolfgreenfield.com, respectively.

dispositive of whether reasonable measures were employed.[3] If there ever were a dispute that resulted in litigation, the onus would be on the trade secret owner to establish that reasonable measures were taken. If a company never shares business-critical information, then there will simply be nothing to litigate – always a best practice.

Limit What Information Is Disclosed

The best way for a company to protect its trade secrets is simply not to disclose them in the first place (both inside and outside the company). There is a simple reason Coca-Cola has been incredibly successful at protecting its secret recipe: only a few people within the company have the recipe and the company does not disclose it to anyone outside the company, regardless of the existence of an NDA.

A best practice is for the policy to also set forth what confidential information the company is willing to accept from others.

In deciding whether a particular piece of a company's confidential information should be widely disseminated within the company or disclosed to others outside the company, management should ask what would happen if a competitor gained unrestricted access to that piece of information. If such access would mean the end of the business, the company should consider adopting a policy that strictly limits access to that information.

Limit What Information Is Accepted and Who Receives It

A best practice is for the policy to also set forth what confidential information the company is willing to accept from others. For example, if an outside party discloses information that it considers confidential that either forms the basis of a new innovation made by the receiving company or that overlaps with developments the receiving company was contemporaneously making, the receiving company may be precluded from monetizing those innovations. In that example, the receiving company could be precluded from monetizing an innovation if doing so would necessarily result in the impermissible disclosure of the other party's confidential information. Or, if there is overlap between the outside party's information, it may make it challenging for the receiving company to establish it independently developed the information. For these reasons and others, many companies refuse to accept creative ideas on a confidential basis.

Another strategy is to sequester the outside party's confidential information to a designated individual who is not part of any product development team. That individual can review the information, decide whether it will impact future expansion of the receiving company's business, and decide whether to return the information to the outside party or pass it along to others in the company. A log should be kept recording receipt of all outside party confidential information listing what action was taken with each piece of information, as discussed further below.

ESTABLISH AT LEAST REASONABLE MEASURES OF PROTECTION

To successfully protect confidential information or a trade secret in court, the owner of the information must establish that it made at least "reasonable efforts to maintain the secrecy of the information." While that may be a low bar in some jurisdictions, best practices aim higher to stay out of litigation altogether.[4] What follows are a few examples of such measures.

Non-Disclosure Agreements

Creating an NDA is usually the first place to start in any exchange of confidential information because it lays out the parties' expectations of what information is to be exchanged, for what purpose and term, how the confidentiality of that information is to be protected, and the disposition of the information at the end of the relationship. Thus, all of the remaining measures of protection below should be considered before crafting an appropriate NDA.

One-Way Versus Two-Way

NDAs are typically structured in one of two formats: one-way NDAs or mutual (two-way) NDAs. In a one-way NDA, information is disclosed by one party, and the receiving party is bound to protect that information. In a mutual NDA, both parties

receive, and mutually agree to protect, the other's confidential information.

One-way NDAs are generally easier to negotiate because there is only one disclosing party and one receiving party, and the burdens on each are distinct. Mutual NDAs are more difficult; because each party is both sending and receiving confidential information, the provisions tend to cut both ways. For example, a broad definition of confidential information will protect the disclosing party, but it could also impose onerous obligations on the receiving party.

Marking Requirements

The NDA should set forth what is and is not confidential information, and protocols for how to identify such information.

No marking: One approach is agreeing that any information that is not publicly available is deemed to be confidential. While this makes things easier for the disclosing party, it can be onerous on the receiving party, which then has the burden of determining if the information it has received is publicly available. This also makes things more difficult for a receiving company's employees to make individual decisions as to how to treat any one piece of information – the risk of inadvertent disclosure goes up considerably.

Marking required: Another approach is that the disclosing party must either label confidential information as such, or if disclosed orally, confirm in writing that what was disclosed was confidential. The benefit to this is it significantly reduces the burden on the receiving party. The drawback is that the disclosing party must be diligent in labeling its own confidential information as such and following up after phone calls and meetings with written memos identifying what aspects of the discussions the disclosing party considers confidential. While marking confidential information as such is a best practice regardless of whether marking is strictly required under the NDA (as discussed below), it is in the disclosing party's best interest to tailor the NDA such that any errant failure to mark is not fatal to keeping the information confidential.

Marking and prior agreements: Still another option is to not only require labeling and documentation of oral communications, but also to set forth in the agreement exactly what confidential information each party anticipates disclosing. Taking this step establishes expectations at the outset of what each party will be providing and receiving and lessens the risk that the outside party will provide information the company would rather not receive.

How to Prove Information Is Not Confidential?

Any well-drafted NDA will provide exclusions as to what is not considered confidential, even if it is labeled as such. Exclusions may include information already in possession of the receiving party or independently developed, but careful consideration must be given to how that is established. How much evidence must the receiving party provide to demonstrate it was already in possession of or that it independently developed the information? Is documentary evidence required? The answers to these questions should be agreed to in writing.

Restrictions of Use

The NDA should identify the purpose of the exchange of confidential information and restrict the use of the confidential information only to that specific purpose. Failing to restrict the receiving party's use of a disclosing company's information can often be as fatal as failing to restrict the receiving party's disclosure of that information, especially when the receiving party is already in a position to commercially exploit the disclosing company's trade secrets and other confidential information.

Ownership of Further Innovations

If the purpose of an NDA is for evaluating a possible joint development opportunity, it is ideal if neither party makes any new inventions or other intellectual property ("IP") as part of the evaluation process. But this is not always practical or possible. Accordingly, it is often best if the parties agree in advance who will own any IP that is created through the use of the disclosed confidential information.

Term of Disclosure & Term of Protection

The term of an NDA refers to both how long each party plans to exchange confidential information (sometimes referred to as the term of disclosure) and how long each party agrees to protect the other's confidential information (sometimes referred to as the term of protection). Establishing indefinite confidentiality obligations in a one-way

NDA is generally favorable for the disclosing party. But indefinite confidentiality obligations cut both ways in a two-way NDA.

Typically, the term of disclosure of the NDA is intimately connected with its purpose. If two parties need to exchange confidential information to understand whether they want to pursue a joint development effort, the term of disclosure of the NDA may be relatively short.

On the other hand, if the parties know that a long-term collaboration is certain, then a longer term of disclosure is more appropriate. Generally, a receiving party under the NDA should include a provision that allows it to terminate the term of disclosure at will, in case it decides it no longer wishes to receive confidential information from the other party.

Even after choosing an appropriate term of disclosure for the agreement, careful consideration should be given to the term of protection. While most company confidential information becomes stale after a few years, and the risks of it being publicly disclosed diminish over time, that is not true of trade secrets, which can last forever if proper protections are put in place. If the disclosure of a trade secret or other highly valuable confidential information is absolutely necessary and contemplated, then the NDA must be structured such that the receiving party has a duty to maintain the confidentiality of such information indefinitely. As a judge in New York explained, a "number of courts have denied trade secret protection where allegedly confidential information has been revealed to third parties . . . where the information was disclosed under a non-disclosure agreement with only a limited duration."[5] Importantly, it is undesirable to the disclosing party for the term of protection to be unilaterally terminable by the receiving party.

Confidentiality and Trade Secret Labels

Regardless of whether the NDA requires marking or not, it is a best practice to mark all confidential information as such (both within the company and when such information is disclosed outside the company) because it helps prevent its inadvertent disclosure. For example, marking all confidential information appropriately when it is disclosed to an outside party under an NDA, regardless of whether such marking is expressly required under the NDA, makes it more difficult for the receiving party to argue it did not know the information was confidential. Internal marking of confidential information provides similar benefits in that no individual employee needs to make any decision as to the confidential nature of the information – it either has a label or it is not confidential.

But be careful not to over mark. All companies will have at least some internal information that is also available to the general public. While it is better to err on the side of caution, avoid the urge to mark a document as confidential when it is clearly not. Selective marking shows that the practice was deliberate, and not boilerplate.[6]

Documentation / Logbooks

A best practice is to create a running log of every piece of confidential information that is disclosed to an outside party: physical documents, physical samples, electronic documents, and memoranda documenting oral disclosures. This log can take many forms, but a simple method is simply to save a copy of each email, document, transmittal letter, or memo produced in a folder with the date it was produced for each third party to which the company provides confidential information. The goal is to be able to, in the future and without too much effort, determine what was disclosed to an outside party, whom at the outside party it was disclosed to, and when it was disclosed.

Establishing a policy is a good first step, but effectively training employees on it is also important.

Another best practice is to create a running log of every piece of confidential information that is received from an outside party. Preparing memoranda documenting oral disclosures, including if no oral communications were made beyond what was disclosed in the outside party documents is also helpful. This prevents an outside party from stating it disclosed something orally when it did not. If a dispute later arises, the company would be able to point to its memoranda and the outside party's lack of response.

Limit Access

Limiting the number of people who are authorized to send and receive confidential information

is a best practice because it better ensures all company policies with respect to confidential information are properly followed. Allowing a large number of employees to distribute confidential information increases the risk that something is distributed that should not be, or that something is improperly marked or otherwise in a manner inconsistent with company policy. Similarly, the more employees that have access to outside party confidential information, the more likely that information will not be properly protected or logged.

Employee Training

Establishing a policy is a good first step, but effectively training employees on it is also important. A best practice is to communicate the policy to existing employees, documenting the training in writing by at least having an attendance sheet to show who was trained on the company policy and when. Periodic (annual or biannual) training on the company policy prevents employees from forgetting their obligations.

Another best practice is asking prospective employees if they have any existing NDAs with prior employers before making an offer of employment, and then asking for copies of the NDAs and retaining them in the employee's records if hired. As part of the onboarding process, remind employees to abide by prior agreements and have them acknowledge in writing that they will do so. And do not forget to train new employees on the company's policies governing confidential information and trade secrets. As with existing employees, document the training by having employees sign attendance acknowledgements.

Require NDAs

Requiring employees to sign NDAs is just as important as having them in place with outside parties, such as any vendors, contractors, or others who must be given access to the company's confidential information. Requiring visitors to sign NDAs if they are to be given access to confidential information is another best practice, as is escorting the visitors at all times during their visits, and keeping them away from areas that will expose them to confidential information, unless there is a clear need for them to access it.

Secure Storage / Passwords

A best practice is to electronically store information in an encrypted and password protected system that automatically logs which authorized users access the information and when. For trade secrets, restrictions should be put in place that prevent the copying or printing of the information without authorization.

For physical storage, while at least one court has held that a "closed file drawer" is enough,[7] a best practice is to lock up trade secret information, with only designated persons having keys. For communal storage not controlled by a single person, a best practice is to keep a log to document when items are removed or copied, by whom, and for what purpose.

Exit Interviews

Conducting an exit interview of any employee with access to confidential information or trade secrets that leaves the company is another best practice.

Remind the employee of his or her obligations under the NDA the employee signed, request the return of any confidential information the employee may have, and collect any computers, electronic devices, keys, etc. that provided the employee access to confidential information.

Ensure that any outside party confidential information is removed from any of the departing employee's personal electronic devices.

Conduct an independent review of that employee's activity in advance of the exit interview with respect to accessing confidential information, looking several months prior to the employee's announcement of his or her departure, and question the employee if there is any activity outside of what would be normally expected.

Finally, document that the exit interview occurred, what was discussed, and that the employee was reminded of his/her nondisclosure obligations.

Audits

Another best practice is to conduct periodic audits to ensure that company policies are being followed – both at the company itself, and consider demanding audit rights in the company's NDAs with others to check up to see that outside parties are protecting the company's confidential

information in the way it agreed. Having a policy is meaningless if it is not being followed.[8]

Document Destruction

Quite a number of trade secret misappropriation claims fail because owners of confidential information never ask the recipient to return or destroy it after the term of the NDA has expired or after the business relationship has ended.[9] When a relationship ends with an outside party, a best practice is to remind the outside party of the NDA, and of the terms requiring return or destruction of the company's confidential information. Here, the log of what was disclosed comes in handy, as the company will have a readily available list of what documents or information was disclosed. Request a certification that all of the listed information was destroyed and keep the outside party's certification of destruction as the final entry in the disclosure log for that party.

Regardless of whether an outside party similarly asks for return or destruction of its confidential information, a best practice is to destroy all copies of that party's confidential information except for one file copy in case the company needs to refer to it to defend against a misappropriation claim. Prepare and maintain a list of employees who were exposed to the outside party's confidential information based on the emails that were saved. Ask these employees to search their personal files and email repository and to delete any files, emails, or other materials that contain the outside party's confidential information and report the results of their search. Save those emails. After searching for and deleting any copies (except for a file copy), document the destruction in a memo and keep that as the final entry in the log of information received from that outside party.

CONCLUSION: FOLLOW THROUGH ON THE PLAN

In this age of constant communication in various forms – from Zoom to online collaborations to phone calls, texts and emails – formulating and implementing a rigorous plan to protect confidential information and trade secrets is especially important. Collaborating with companies and vendors outside an organization requires particular vigilance. Safeguarding a company's confidential information internally and in work with outside parties can avoid costly losses, litigation and dilution of the value of the company's IP.

While not all of the above measures need to be taken in all cases for all types of information, each should be discussed by a company's stakeholders to strike the right balance between meeting business needs and protecting the company's IP. And above all, once a company puts a plan in place, stick with it. Following through on the plan is the single top tip for protecting the company's confidential information when sharing it with others.

Notes

1. Confidential information is any information that a company wants to keep private. Trade secrets are one type of confidential information that, while definitions vary, is something that is not generally known in the industry, has commercial value by being kept secret, and is the subject of reasonable measures of protection. This article will refer to confidential information generically as encompassing trade secrets.
2. *See Tax Track Sys. Corp. v. New Inv. World, Inc.*, 478 F.3d 783 (7th Cir. 2007).
3. *Silicon Image, Inc. v. Analogix Semiconductor, Inc.*, No. 07-cv-00635 JCS, 2008 WL 166950, at *17 (N.D. Cal. Jan. 17, 2008) (denying a motion for preliminary injunction to protect a trade secret because although NDAs were in place, both the trade secret owner and those to whom the trade secret was disclosed "have sometimes disregarded and failed to respect . . . [the] obligations imposed under NDAs" causing the court to question whether "reliance on NDAs to protect its own confidential information was reasonable").
4. *See Learning Curve Toys, Inc. v. PlayWood Toys, Inc.*, 342 F.3d 714 (7th Cir. 2003).
5. *Structured Cap. Sols., LLC v. Commerzbank AG*, 177 F. Supp. 3d 816, 835 (S.D.N.Y. 2016), *citing Silicon Image,* 2008 WL 166950 at *17; *DB Riley, Inc. v. AB Eng'g Corp.*, 977 F. Supp. 84, 91 (D. Mass. 1997); *ECT Int'l, Inc. v. Zwerlein*, 228 Wis.2d 343, 355-56 (Wis. Ct. App. 1999) (affirming dismissal of misappropriation claim where confidentiality agreement specified that information was to be kept confidential for only one year, thereby "manifest[ing] [plaintiff's] intent that after one year there was no need to maintain the secrecy of any sensitive and confidential information").
6. A boilerplate statement that a document "may contain" confidential information "bears no relevance, as a matter

of law, as to whether . . . appropriate steps to safeguard . . . alleged trade secrets" have been taken. *Sortiumusa LLC v. Hunger*, No. 3:11-cv-1656-M, 2013 WL 11730655, at *11 (N.D. Tex. Mar. 31, 2013).

7. *Elmer Miller, Inc. v. Landis*, 253 Ill. App. 3d 129, 130 (1993) (finding reasonable measures to protect customer files when they were "kept in a closed file drawer").
8. *Silicon Image,* 2008 WL 166950 at *17.
9. *See CMBB LLC v. Lockwood Mfg., Inc.*, 628 F. Supp. 2d 881 (N.D. Ill. 2009).