August 05, 2019
FEATURE

Trade Secret Diligence in M&A

James Pooley

When one company looks at buying another, the potential buyer engages in a "due diligence" process designed to help it fully understand the relevant risks and opportunities before the deal is done. In today's digital economy, most business assets are intangible, and so intellectual property (IP) is among the most meaningful of the variety of issues that an acquirer needs to examine. But while most due diligence checklists include dozens of questions pointed at the target company's patents, trademarks, and copyrights, trade secrets get relatively little attention, often limited to a single request to confirm that the target has some system in place to protect its secrets from unauthorized disclosure.

This light touch on trade secrets, compared to the other forms of intellectual property, can seem bewildering when you consider that secrecy has been shown repeatedly to be the preferred method of protecting commercial innovation.[1] Moreover, with so many companies turning to data collection and analysis as a way to enhance their competitive position, one would think that trade secrets should get top billing in any assessment of a commercial transaction. That it frequently doesn't may reflect the roots of trade secrets in state common law, distinct from the registered IP rights, which can be counted and more easily valued. Even though we now have legislation at the state (Uniform Trade Secrets Act) and federal (Defend Trade Secrets Act) levels, trade secrets may still seem relatively mysterious to many of the corporate lawyers who lead due diligence efforts in connection with acquisitions. Or those lawyers may just assume that these issues are being handled by the company's IP specialists.

Information as an Asset

Some industries and companies typically pay close attention to their most valuable secrets, due to the nature of their businesses. Examples include chemical manufacturers, biotech companies with their heavy emphasis on R&D, and to a certain extent software companies that increasingly locate their core algorithms in a private cloud, where customers can use the tool but not look inside. But a lot of what makes any business valuable consists of more dispersed technology, including knowing what not to do ("negative know-how") and insights drawn from data analytics that in turn drive marketing strategies.

Based on anecdotal experience, it seems that, with some exceptions where the acquirer pays very close attention, there is often a disconnect between the perceived importance of information assets in the abstract and how they are actually treated in the context of planning, investigating, and executing business combinations. Even where these assets might seem not to matter very much, as when the acquirer plans an "acquihire" (buying the company just to get its smart employees), there is still reason for concern, since trade secrets reside largely in the heads of individual actors, who may or may not stay around after the deal is done.

All businesses face risks in connection with their information assets, more or less constantly. That's a necessary result of the trend toward "open innovation,"[2] coupled with the fact that the systems used for storage and communication of data allow wide access to hundreds or thousands of individuals and are to one degree or another insecure. A lot can be done to manage those risks on an ongoing basis, but the potential acquisition presents a uniquely fraught circumstance compared to other relationships because the parties' interests at the outset are not necessarily aligned, and the time frame for dealing with some very complex and challenging issues is often quite short. Both sides in the deal must confront significant risks resulting from the understandable anxiety that each experiences (or should experience) from sharing or receiving highly confidential information.

Risks to the Target

Let's first consider the target company. Classically, the biggest hazard faced by the target is the almost existential risk that it will expose its core secrets to a suitor who ultimately walks away from the deal and goes into direct competition. And while that fear is legitimate and should inform any number of protective strategies, it may make more sense to first recognize a somewhat counterintuitive problem: the risk of success. By this I mean that if the deal goes through, the target will have to provide very extensive "reps and warranties"—essentially guarantees about the ownership and security of its information assets and freedom from third-

party claims. Here is an example, cast in the typically overburdened prose of commercial transaction documentation:

> The Company and each of its Subsidiaries have taken all commercially reasonable measures to protect and preserve the confidentiality of any Trade Secrets that comprise a material part of the Company IP. To the knowledge of the Company, all use and disclosure of Trade Secrets owned by another Person by the Company or any of its Subsidiaries have been pursuant to the terms of a written agreement with such Person, or such use and disclosure by the Company or any of its Subsidiaries was otherwise lawful.

The prospect of signing on to these guarantees represents a challenge because the target needs to start preparing for this responsibility very early in the process, by revisiting its trade secret protection program, as well as its compliance with outstanding confidentiality agreements. Of course, this can also be viewed as an opportunity to enhance trade secret governance, no matter the outcome of the proposed acquisition. IP counsel advising the target company can be very helpful in directing this analysis, including identifying specific areas of risk and setting priorities for management action.

But the deeper and more consequential concern is that the transaction will not come to pass, and the purported acquirer turns into a competitor made more capable and threatening by virtue of having had access to the target's secrets. Here too, reducing this dimension of risk begins with getting the house in order regarding trade secret management. The first step in taking adequate precautions is to know what trade secrets you have, how they are represented (in code, in process documents, in the head of the fellow who operates the production line, etc.), and what their value is to the company. The latter can be an expression of how much they contribute to profitability due to increased efficiency, for example, or of the damage that would be caused if the information fell into the hands of a competitor. Either way, addressing in a disciplined way the relative value of the target's major categories of information assets will inform the extent of risk taken in the coming negotiations over how much of it the suitor will be allowed to see and under what conditions, as well as perhaps the financial terms of the hoped-for acquisition.

The starting point for disclosure must be a robust nondisclosure agreement (NDA) by which the potential acquirer acknowledges the confidential nature of the process and promises not to disclose or use any confidential information other than to evaluate the possible deal. This contract has to be negotiated at the outset, separately from the terms of the eventual transaction (although

executing a concurrent letter of intent is quite common), and before any secrets are exposed. From the target's perspective, the NDA needs to include a broad definition of "confidential information," allowing for only the standard exceptions for information that is publicly known, developed by the recipient independently of its exposure to the secrets, provided properly by a third party, or already in the recipient's possession (the latter should be limited to what can be demonstrated by contemporaneous records).

To the extent possible, the target should resist agreeing to a "residuals clause," which removes from coverage any information that is "retained in the unaided memory" of the people who are to have access to the target's secrets. Although there may be good reasons for the potential buyer to want such protection for itself (see discussion below on this point), the practical effect can be to grant a license to the target's secrets. Not only does this open up the possibility of unfair competition from the buyer if the deal doesn't go through; it also imperils the general enforceability of the target's secrets as to others, because they can claim that the information has not been the subject of "reasonable efforts" to protect it, a necessary element of establishing trade secret rights.

Another significant provision from the perspective of the target addresses what to do about verbal disclosures of secret information. The buyer's NDA may limit confidential information to what is contained in documents that are prominently designated as confidential. But the due diligence process normally includes interviews in which additional sensitive information may be revealed. It is important that the target at least have the opportunity to identify this information in a written communication within a specific time following disclosure. And speaking of time, the target should consider very carefully any attempt to limit the term of the recipient buyer's confidentiality obligations. Again, such a limitation (typically three to five years) is rational and reflects the other party's interest in avoiding the administrative burden of perpetual compliance. But as with the residuals clause, putting a limit on the period of confidentiality can have the effect of granting a license when the period expires; so the target must be comfortable that none of the shared information will remain valuable after that time.

Whatever the terms of the NDA, there will remain some risk that information will be misused beyond the target's awareness or ability to prevent. Therefore, it also needs to focus on the process of disclosure, to ensure that information is only transferred when and to the extent that it needs to be. In general, it is a good idea to use "progressive incremental disclosure," starting with an exchange of nonconfidential data, and then working gradually through increasingly sensitive information as trust and confidence between the parties build. Each stage thereby provides a

basis for understanding the value and risk of moving to the next stage. For some highly sensitive information, special restrictions might include limiting disclosure to named individuals or under supervision without the ability to copy or take notes. And it may even be possible to negotiate for a limited disclosure of certain items, or certain details, leaving full disclosure to occur only after closing. Sometimes the acquirer will accept such terms because it has been able to make a sufficient assessment based only on partial access and the deal otherwise has enough momentum to justify it.

Risks to the Buyer

In contrast to the target, the buyer's major risk, besides overlooking some aspect of the target's data assets, is in its exposure to information that might be relevant to the company's own R&D or other business transactions. These concerns for potential "information contamination" are most acute when the company has an existing plan to develop related technology in-house but wants to compare that possibility to what it might be able to acquire outside. This is known as the "make vs. buy" conundrum, and it is fraught with hazards.

The reason we refer to this situation as a conundrum is that the potential acquirer has separate interests that tend to compete with each other. For example, it wants to know as much as it can about the target's technology and strategies, so that it can adequately assess the transaction. But at the same time, acknowledging that the deal may not happen, it also wants to protect its own freedom to operate and so would like to keep exposure to the target's secrets to a minimum. This ambivalence is sometimes compounded by different internal agendas, typically because of the related internal development program, whose leaders naturally would like to win the "make vs. buy" contest. This can lead to their breaching the wall between their group and the deal team, as they try to better understand the competition.

The challenge is much greater if no such barrier was erected to begin with. In *Nilssen v. Motorola*,[3] the court denied summary judgment on the defendant's claim that its competing product was developed independently of the target's technology, because some of the supervisors of the internal project had attended due diligence meetings with the target company's engineers. As the court explained, "the placement of key employees in a position where they might assimilate a trade secret permits an inference of misappropriation."[4] The point had been made even more forcefully by the Federal Circuit in *Roton Barrier v. Stanley Works*,[5] in which the prospective buyer had tried to argue that the personnel exposed to the target's secrets did not meaningfully participate in the internal development project, but merely supervised others who did the work.

The court rejected the argument as "disingenuous." It also declined to recognize as independent the work of a third party hired by the buyer to manufacture its competing product, because it had been given instructions by those who had access to the target.

Occasionally the breach occurs in a narrower but equally dramatic way, as when the buyer's outside patent attorney is tasked with reviewing the target's unpublished patent application to assess its strength. This was the situation in *X-IT Products v. Walter Kidde*,[6] in which the court denied summary judgment to the defendant because the draft claims in the application were deemed to reflect the target's confidential assessment of the most protectable features. The attorney had passed on this information, together with a list of cited prior art from the application, to an associate who was working on an application for the defendant in a related field. Although the defendant managed to demonstrate independent work in every other respect, this leakage was enough to deny summary judgment.

Transgressions like these can have serious consequences beyond exposure to a damage award. In *Den-Tal-Ez v. Siemens*,[7] the buyer falsely assured the target that it was no longer interested in acquiring a competitor, while in fact it was conducting meetings in parallel and ultimately chose the competitor. Having been exposed to the plaintiff's manufacturing facilities and technical know-how, the buyer was enjoined from completing its intended acquisition, or acquiring any other competitor, for a period of three years. The injunction was affirmed based on a theory of threatened misappropriation, which the court deemed "inevitable."

While some of these mistakes are operational, the potential acquirer's first line of defense against liability is an NDA carefully constructed to cabin its exposure. Ideally, the contract should limit protected information to that which is provided by the target in writing and clearly marked as confidential. If verbal disclosures are to be permitted, they should be effective only if confirmed in a specific writing within a brief period. (Note that someone on the recipient's side should be tasked with receiving and verifying the contents with those involved in the disclosure.)

Whether or not the prospective buyer is engaged in development of a competing product or service, it is wise to include in the NDA an acknowledgment that it may be so engaged, and that there have been no representations of exclusivity, the buyer being free to consider the acquisition of alternative businesses or technologies. The most reliable way for the buyer to protect its freedom is by insisting on a "residuals clause," typically some variation of the following:

> Discloser agrees that the disclosure of Confidential Information to Recipient shall not impair the right of Recipient to engage in its business, including the development of products and services that are competitive with that of Discloser, provided that Recipient does not breach this Agreement. Therefore, it is agreed that Recipient may use Residuals for any purpose. "Residuals" means any information retained in the unaided memories of the Recipient's employees who have had access to the Discloser's Confidential Information pursuant to this Agreement. An employee's memory is unaided if the employee has not intentionally memorized the information for the purpose of retaining and subsequently using or disclosing it in violation of this Agreement.[8]

Other important provisions of the NDA include setting a time when confidentiality will expire (this may prompt push-back from the target, but particularly if there is no residuals clause the administrative burden of perpetual management of the exposure can be a very legitimate concern) and a choice of law and forum (critical for cross-border deals). A requirement to arbitrate disputes may also be helpful, especially as a way to ensure confidentiality.

No matter how complete and robust the contract governing the transaction, effective due diligence requires very close management of the process. Generally speaking, complete, documented separation should be maintained between those who have access to the target's secrets (the "clean team") and those who are engaged in internal development. For particularly sensitive situations, such as where the company has an ongoing project that is directly competitive, it may be wise to employ a third party to handle the diligence, or the relevant portion of it, and to report back only their recommendations. And there may be some information that is so highly confidential that the target is unwilling to provide access at all before closing. This then becomes a matter of assessing the risk, which may be mitigated to an extent through representations and warranties in the transaction documents.

Other Due Diligence Considerations

Having identified, allocated, and controlled the risks as appropriate, diligence proceeds with the objective of learning as much as possible about the target's trade secrets and how they are protected and deployed. Among the documents to be examined should be employee and consultant confidentiality and invention assignment agreements, third party NDAs and related contracts, policies and procedures regarding trade secret protection, training programs, records of R&D, and licenses or other agreements reflecting ownership and control (including the ability to transfer to the acquirer), such as joint development or funding relationships.

Examination of the target's trade secret protection program is not about checking a box, but should be as thorough as necessary to assess whether it at least meets the "reasonable efforts" element of secrecy as defined by the Uniform Trade Secrets Act and the Defend Trade Secrets Act.[9] Interpreting that provision, the courts expect the trade secret holder to balance the value of the information against the risk of loss, measured against the cost of various measures that could reduce or eliminate the risk.[10] A good description of this basic risk management approach in practice is provided by CREATe.org.[11]

The due diligence process should also address the following questions:

- What is the provenance of the target's technology? How might it have been tainted by information brought to the company by employees or through the company's confidential transactions with other entities?
- To what extent have the target's employees come from competitors? Have any warning letters been received? What are the target's recruiting and onboarding processes designed to avoid contamination by third-party data?
- Has the target experienced any trade secret claims or threats of disputes? Have any disputes resulted in settlement agreements with ongoing obligations?
- Can the target reliably vouch for the ownership of its trade secrets, based on proper assignments by employees and third parties involved in development? If any secret information has been licensed in, can it be assigned?
- What efforts have been made to capture and document know-how in the heads of key employees who might leave as a result of the acquisition? Are there noncompete agreements in place, or can they be obtained?
- How has the target managed compliance with its obligations under the various NDAs it has entered into with third parties?
- To what extent has the target developed a "culture of confidentiality" in the workplace that encourages good IT security hygiene and compliance with access controls and other confidentiality procedures?
- To what extent are the target's trade secrets exposed to actors in foreign jurisdictions?

Post-Acquisition Integration Plan

Finally, assuming that the acquisition proceeds, the buyer should have created a thoughtful plan for integration of the target's workforce. Corporate cultures and practices around treatment of confidential information vary greatly. Employees at a very small company may not be used to the controls required in a more hierarchical organization. Even companies of equivalent circumstances may have established different approaches. The integration plan should combine the best information access and security measures from each, just as with other aspects of their operations. Whatever the decision regarding ongoing structures, the surviving company should institute a rigorous and ongoing training program, with regular follow-up.

Endnotes

1. *See* John E. Jankowski, *Business Use of Intellectual Property Protection Documented in NSF Survey*, Nat'l Sci. Found. (Feb. 2012), https://wayback.archive-it.org/5902/20150628145722/http://www.nsf.gov/statistics/infbrief/nsf12307/nsf12307.pdf.

2. "Open innovation" is the tendency of modern business to innovate through collaborations and acquisition, rather than just internal development. *See Open Innovation*, Wikipedia, https://en.wikipedia.org/wiki/Open_innovation (last modified May 18, 2019).

3. Nilssen v. Motorola, Inc., 963 F. Supp. 664 (N.D. Ill. 1997).

4. *Id.* at 683.

5. Roton Barrier, Inc. v. Stanley Works, 79 F.3d 1112, 1118 (Fed. Cir. 1996) (observing that "parties at Stanley instrumental in reviewing Roton's manufacturing facilities and financial data were the same people placed in charge of developing" Stanley's product).

6. X-IT Prods., LLC v. Walter Kidde Portable Equip., Inc., 155 F. Supp. 2d 577, 643, 646–47 (E.D. Va. 2001) ("[T]he information contained within X-IT's patent application represented X-IT's 'blueprint' of how to exclude others from copying its ladder.").

7. Den-Tal-Ez, Inc. v. Siemens Capital Corp., 566 A.2d 1214, 1231–32 (Pa. Super. Ct. 1989).

8. A residuals clause is not a free pass to use confidential information. In *Space Data Corp. v. Alphabet Inc.*, No. 16-cv-03260-BLF, 2017 U.S. Dist. LEXIS 222326, at *9 (N.D. Cal. Dec. 18, 2017), the

court denied a motion to dismiss a claim of misappropriation based on the potential acquirer's photographs taken of the target's facilities during the due diligence process.

9. Unif. Trade Secrets Act § 1(4) (amended 1985), 14 U.L.A. 538–39 (2005) ("efforts that are reasonable under the circumstances to maintain . . . secrecy"); 18 U.S.C. § 1839(3)(A) ("reasonable measures to keep such information secret").

10. *See, e.g.*, *In re* Innovative Constr. Sys., Inc., 793 F.2d 875, 884 (7th Cir. 1986); *see also* Restatement (Third) of Unfair Competition § 43 cmt. c (Am. Law Inst. 1995).

11. *See* Ctr. for Responsible Enter. & Trade (CREATe), Protecting Trade Secrets from Cyber and Other Threats (2018), https://create.org/resource/reasonable-steps-to-protect-trade-secrets-leading-practices-in-an-evolving-legal-landscape/.

ENTITY:

SECTION OF INTELLECTUAL PROPERTY LAW

TOPIC:

INTELLECTUAL PROPERTY

Authors

James Pooley

James Pooley is a Silicon Valley lawyer focusing on the law and management of trade secrets, as an advocate, advisor, and neutral.