How (Not) to Destroy Your Trade Secrets

New York Intellectual Property Law Association
Fall Patent CLE Series
November 18, 2021

Rachel Blitzer
Skadden, Arps, Slate,
Meagher & Flom LLP

Laura Chubb
Haug Partners

Mark Schildkraut
Becton, Dickinson and Company

How (Not) to Destroy Your Trade Secrets

The Basics

- ❑ Trade Secret vs. Confidential Considerations
- ❑ Identifying Your Trade Secrets
- ❑ Failing to Take Reasonable Measures to Protect
- ❑ Every Conceivable Measure Not Required
- ❑ Inconsistent Application of Reasonable Measures
- ❑ Overly Aggressive Confidentiality Requirements

The Workplace

- ❑ Poor Workplace Practices
- ❑ Balancing "Big Brother" Policies with Employee Monitoring
- ❑ Open Zoom Calls
- ❑ Lax Work From Home Procedures

Some Unique Circumstances

- ❑ Displaying Before Thousands
- ❑ Passage of Time
- ❑ Including Trade Secret in Published Patent (Even If Patentee Is Not Rightful Trade Secret Holder)
- ❑ Software and Source Code Issues
- ❑ Industry-Specific Watch-Outs

Agreements

- ❑ Insufficient NDA Terms
- ❑ Joint Venture Agreements

Litigation

- ❑ Failure to Sufficiently Describe Trade Secret
- ❑ Protective Orders / Motions to Seal
- ❑ Emergency Relief / TRO Challenges

How (Not) to Destroy Your Trade Secrets

By: William Marsillo, Boies Schiller Flexner LLP[1]

Analyzing "do's and don'ts" for protecting trade secrets must account for the context in which that analysis is done. The COVID-19 pandemic has presented exceptional and unprecedented challenges in many areas of how companies do business, including how they can protect valuable confidential information and trade secrets.

As a result of the pandemic, entire workforces were forced to work remotely, which required accessing trade secrets from home, transmitting work product containing trade secrets over home WiFi and other connections, and discussing trade secrets on virtual meetings and teleconferences. In some cases, our remote connections led to the disclosure of confidential information or trade secrets to third parties outside of normal procedures.

The dislocations arising from the pandemic have challenged our usual ways of assessing trade secrets. Concepts like whether "reasonable measures" were taken to protect a trade secret or whether a trade secret was "properly identified," are likely to be tested over the next few years as litigation continues to surface about the adaptations companies were forced to make in the face of the COVID-19 health crisis.

In this context, it is even more important to consider changes that likely will be with us for the foreseeable future and focus on steps to take to avoid compromising a trade secret—How (Not) to Destroy Your Trade Secrets.

1. Use reasonable measures to protect trade secrets in a remote environment

A trade secret owner has the duty to be vigilant in protecting its secrets. Indeed, in order for confidential information to be considered a trade secret, the trade secret owner must use reasonable measures to maintain secrecy. *E.g., Abrasic 90 Inc. v. Weldcote Metals, Inc.*, 364 F.Supp. 3d 888 (N.D. Ill. 2019) (where plaintiff "did virtually nothing to protect that information to preserve its status as a trade secret," court concluded that "[plaintiff's] conduct was consistent not with its assessment that the information at issue would be of significant value to a competitor, but rather with [defendant's] assessment that it 'would have negligible value' to a competitor.").

Courts assess what efforts are reasonable "under the circumstances" based on the nature and value of the trade secret information sought to be protected, the extent to which it is known outside of the business, the extent to which it is known by employees and others involved in the business, the extent of measures taken to guard the secrecy of the information, the amount of effort

[1] William Marsillo is a partner of Boies Schiller Flexner LLP

or money expended in developing the information, the ease of theft, the extent of the threat of theft, and the particular field of knowledge or industry.[2]

Of course, what may be reasonable in one context may not be reasonable in another. As one court put it, "taking precautionary measures to protect secrets imposes both direct and indirect costs on the owner of the secret, and thus 'perfect security is not optimum security.'" Security measures need not be extreme and unduly expensive. However, courts expect to see that a business has taken reasonable steps specifically designed to protect the disclosure of its trade secrets above and beyond general protective measures.[3] "Reasonable efforts to maintain secrecy need not be overly extravagant, and absolute secrecy is not required … The fact that a trade secret was successfully misappropriated does not defeat the fact that there were reasonable efforts to maintain its secrecy." *Allergan, Inc. v. Merz Pharm., LLC*, No. SACV11-446-AG, 2012 U.S. Dist. LEXIS 31981 (C.D. Cal. March 9, 2012).

In the new remote workplace environment resulting from the pandemic, what constitutes reasonable measures should be carefully examined. The pandemic prompted ubiquitous use of Zoom, Microsoft Teams, and other collaboration software, all of which became crucial for remote work.[4] Employees, in turn, increased their use of external storage devices to save and access work-related documents. While one expects that employees are just trying to be efficient and have ready access to materials they need to do their job, this practice creates potential problems for companies interested in protecting trade secrets. To minimize the risk of having a trade secret needlessly destroyed, especially in the remote-work setting, employers should consider limiting access to trade secrets to only those persons, groups or departments who really "need to know." E.g., *Epic Sys. Corp. v. Tata Consultancy Services Ltd.*, , Nos. 19-1528 & 19-1613 (7th Cir. Nov. 19, 2020) (examples of steps taken to limit access). For example, an employer could require passwords and secure logins to access corporate networks, particular systems, or specific drives, files, folders or even documents. Employers should also consider using firewalls or other similar software to protect their trade secrets by creating a barrier between their trusted internal network and untrusted external networks, *see, e.g.*, *In Wrap–N–Pack, Inc. v. Eisenberg*, No. 04-cv-4887, 2007 WL 952069, at *9 (E.D.N.Y. Mar. 29, 2007); encrypting particularly high value trade secret information; holding employees to the same standards for protecting company information when working-from-home as when working from the office; disabling USB drives on company laptops to prevent the download and large scale theft of company documents; email monitoring of attachments; and clearly communicating policies and procedures specific to working-from-home.[5]

2. Take measures to properly identify information that is a trade secret

---

[2] *UAB, Inc. v. Ethos Auto Body, LLC*, Index 70850/2018, 2021 N.Y. Misc. LEXIS 4960 (N.Y. Sup. Ct. Mar. 9, 2021).

[3] *Turret Labs USA, Inc. v. CargoSprint, LLC*, , 19-cv-6793, 2021 U.S. Dist. LEXIS 27838 (E.D.N.Y. Feb. 12, 2021).

[4] Zoom's CEO noted that the Coronavirus outbreak will 'change the landscape' of work and communication. GeekWire. URL: https://www.geekwire.com/2020/zoom-ceo-coronavirus-outbreak-will-change-landscape-work-communication/

[5] "'Reasonable Measures' To Protect Trade Secrets At Risk With Employees Working-From-Home Amid Covid-19 Crisis." https://www.quinnemanuel.com/the-firm/publications/reasonable-measures-to-protect-trade-secrets-at-risk-with-employees-working-from-home-amid-covid-19-crisis/

Not all confidential information is a trade secret[6] and companies should take steps to identify the information that they truly regard as a trade secret. That will help not only in ensuring reasonable steps are taken to protect particularly sensitive and valuable information, but also will allow appropriate enforcement steps to be taken, including litigation, should the need arise.

Identification of a company's trade secret is a first step required to bring litigation if needed. To that end, courts have wrestled with the level of particularity needed to define trade secrets to even present a claim of misappropriation. In *Lavvan, Inc. v. Amyris, Inc.,* 2021 U.S. Dist. LEXIS 138887 (S.D.N.Y. July 26, 2021), for example, the court noted how courts are divided with regard to the level of specificity required in pleading the existence of a trade secret. While some courts have accepted relatively general descriptions, others have held that a plaintiff's mere allegation of the existence of general categories of confidential information without any details is insufficient to properly plead a misappropriation claim.[7]

Trade-secret identification is also more critical than ever before because our business environment involves more remote connections than in prior years and transmission of important sensitive information such as business know-how, customer lists, and even HR records to employees' home devices, which creates a substantial risk of the unintended disclosure or misappropriation of trade secrets. Employers should consider more strategic and preventive approaches to securing their trade secrets in this new normal of remote work. For example, marking trade secret information as such or setting up reminders that pop up every time a remote employee logs into the company's systems to act as a notice that the information is a trade secret and must be handled according to the company's policies and procedures. Marking materials as sensitive trade secrets information will help accomplish multiple goals: it can show reasonable measures taken to avoid misappropriation, it can help the victim of a trade secret theft establish willfulness on the part of an unauthorized third-party recipient of the trade secret, and it can help companies clearly and sufficiently present a trade secret enforcement claim to improve their chance of obtaining a remedy for the breach.

3. Carefully consider whether a potential misappropriation requires emergency relief

As companies face the prospect of losing a trade secret, one consideration that should be addressed is whether the circumstances warrant emergency relief from a court, such as through a temporary restraining order or a preliminary injunction. When courts had full accessibility to in-

---

[6] *UAB, Inc. v. Ethos Auto Body, LLC*, 2021 N.Y. Misc. LEXIS 4960 (Westchester County Sup. Ct) (emphasizing that mere knowledge of the intricacies of a business operation does not qualify as trade secret misappropriation, and marketing or other financial information, market strategies, and technical know-how may not be a trade secret if the information is easily ascertainable from non-confidential sources).

[7] *Lavvan, Inc. v. Amyris, Inc*., 20-cv-7386, 2021 U.S. Dist. LEXIS 138887 (S.D.N.Y. July 26, 2021); *Mallet and Co. Inc. v. Synova LLC, et al.*, 20-3584 (3rd Cir. Oct. 15, 2021) (vacating preliminary injunction and remanding because plaintiff provided only categories of what it considered its trade secrets and did not identify them with specificity—i.e., categories such as "formulas," customer purchase orders pricing; "internal discussions of customers' preferences and complaints"; identification of a "supply source for product ingredients;" "internal manuals and procedures" showing how a lab is operated; and "pricing and volume data" are too general)

person conferences, the calculus of whether to seek immediate relief in many cases could have favored filing a motion. However, amid the pandemic, courts closed, court staff was reduced, and court priorities changed as to which matters needed to be addressed promptly. Attitudes about preventing employees from changing jobs in the middle of the pandemic also may have changed, all of which is to say that decisions as to when to go to court and the relief requested must be strategically considered and be consistent with the overall circumstances. It would be counter-productive to rush to court only to lose the motion, potentially get a problematic ruling as to whether the court views the alleged trade secret as a trade secret, and risk leaving an unfavorable impression of the merits of the case.[8]

4. Never have a videoconference or teleconference without a password or other means of limiting access

As we go from one video- or teleconference to another, only to continue the cycle by scheduling still other remote conversations, we can lose sight of the continued need for vigilance in ensuring the confidentiality of our conversations and written communications. We would not display trade secrets on a Times Square screen or to an unintended audience, but we may be doing something comparable by sharing our screen without first ensuring that access to the videoconference was password-protected or otherwise restricted. It will be difficult to explain to a court (or our clients and employers!), and ultimately will likely to be a losing argument, if we organize a videoconference, fail to set a password or other restrictions, and then share a trade secret during the conference in the spirit of collaboration only to have that disclosure destroy the trade secret's value. While this consideration analytically falls within the scope of above Point 1 (Use reasonable measures to protect trade secrets in a remote environment), it is important enough to stand alone. Courts have rejected misappropriation claims where the trade secret owner failed to use security features available on platforms like Zoom. *See Smash Franchise Partners, LLC v. Kanda Holdings, Inc.*, No. 2020-0302, 2020 Del. Ch. LEXIS 263 (Del. Ch. Aug. 13, 2020). That includes taking roll call and removing those who don't belong, *changing* meeting passcodes so that an individual or group with access to one meeting or conversation does not have unlimited access to all meetings and conversations going forward unless that is exactly what is intended.

5. Ensure NDAs and other protective measures cover remote access and are consistently and timely applied

Consistent and timely use of procedures, agreements, and protocols that protect trade secrets remains of paramount importance. For example, when sensitive information is shared with a potential partner, customer, or supplier without first requiring execution of a non-disclosure agreement, designating the information as highly confidential, or taking other actions to restrict access to and use of that information, there is a risk under those circumstances that you will lose the value of that trade secret if you ever seek to protect it in court. The risk includes your adversary pointing to instances in which you have had others sign NDAs before you shared sensitive information (whether or not the same information), which likely will only result in

[8] What Constitutes a Litigation "Emergency" During a Worldwide Health Crisis? By Erik Weibust, Marcus Mintz & Jeremy Cohen on March 26, 2020 URL: https://www.tradesecretslaw.com/2020/03/articles/trade-secrets/what-constitutes-a-litigation-emergency-during-a-worldwide-health-crisis/

making your adversary's argument stronger. That is, by showing that you know how to protect your trade secrets and did so on other occasions will only raise more questions as to why that was not done in this instance. Worse, it could lead to the conclusion that since you know how to protect your trade secrets, you chose not to do so on this occasion, and therefore, the information can no longer be considered a trade secret (assuming it ever was). *BCOWW Holdings, LLC, et al. v. Collins, et al.*, 17-CA-00379, 2017 US Dist LEXIS 142618 (W.D. Tex. Sept. 5, 2017) (denying preliminary injunction where plaintiff did not protect information shared with vendors, noting that plaintiff used NDAs in other instances, which demonstrated that plaintiff knew how to use protective measures but failed to do so in the circumstances before the court).

So, if you have a protocol in place to protect trade secrets that involves, for example, limiting access, password protection, NDA requirements, and visible confidentiality designations, make sure that process is followed at all times. You may want in your NDAs, for example, provisions requiring specific access requirements for specific individuals and to provide that the confidentiality obligations last as long as permitted by law. That, in turn, necessitates training anyone with authority to access and circulate the information so that they know the protocol and follow it religiously.

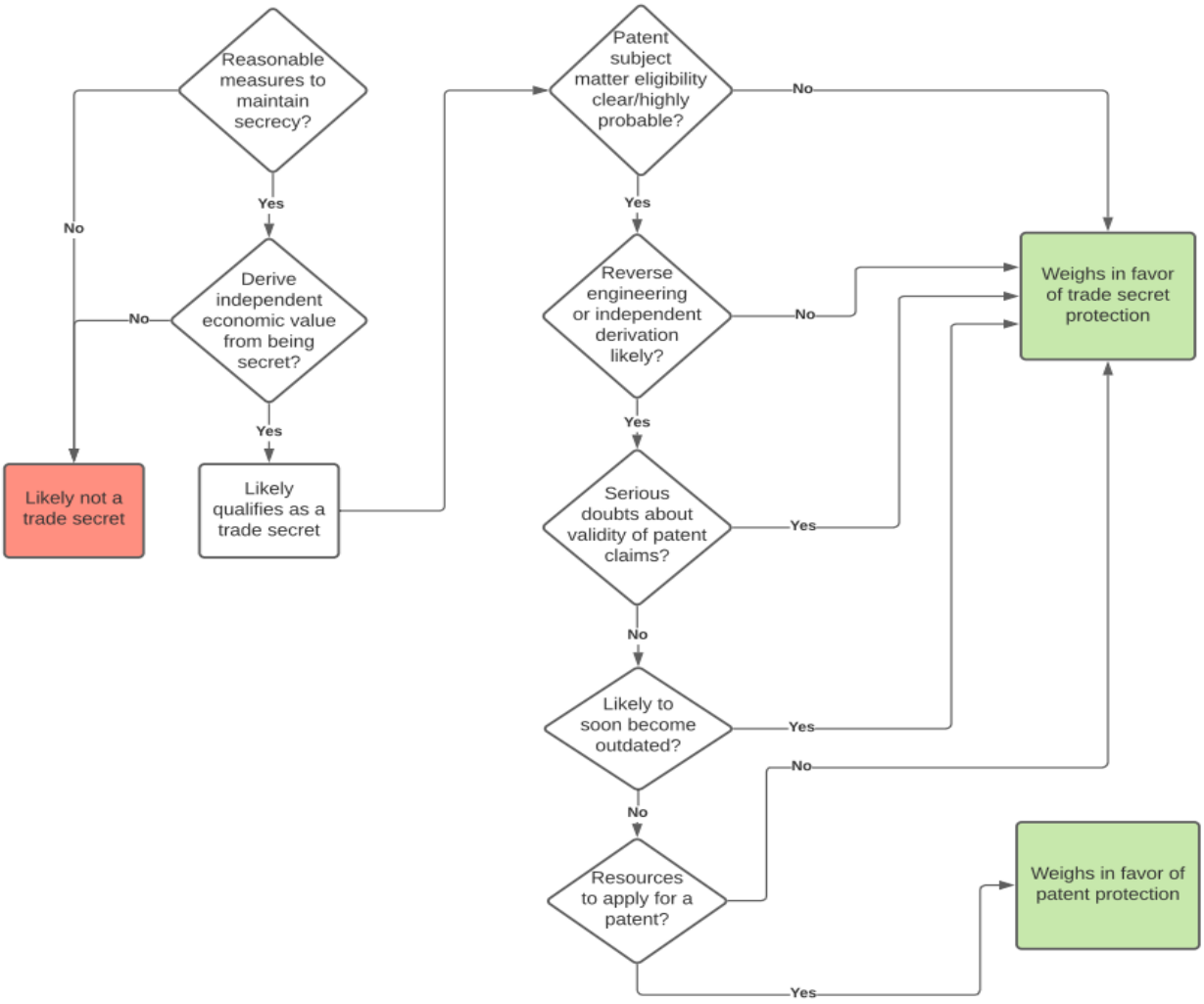
In addition, make sure that process is not only followed but that it is followed from the very beginning of any interactions that may require the sharing of a trade secret. Sharing the trade secret without protections in place only to later try to restrict use of the information may be seen as an insurmountable hurdle for enforcement.

In *SMH Enterprises, L.L.C. v. Krispy Krunchy Foods, L.L.C., et al.*, 20-2970, 2021 US Dist LEXIS 186503 (E.D. La. Sept. 29, 2021), for example, the court granted defendant's summary judgment motion with respect to certain trade secrets because there was no issue of material fact as to whether protective measures (in this case, contractual confidentiality provisions) had been used to protect the trade secret. The initial contract between the parties governing use of a pilot version of the software at issue had no confidentiality provision, even though the amended contract for the full software release contained such a confidentiality provision, that provision excluded information already known to the recipient including the software at issue. "Plaintiff has not introduced any evidence showing that it took any measures to prevent the approximately 17,000 users from disclosing the visible aspects of the [trade secret] to third parties." The plaintiff's last-minute attempt under Rule 56(d) to seek third-party discovery from defendant's partner stores regarding any protective measures they undertook or discovery about the plain meaning of the contracts did not save it from summary judgment.

6. Decide whether trade secret or patent protection is more appropriate under the circumstances, including whether remote work changes your calculus

Deciding whether to protect intellectual property as a trade secret or as a patent involves consideration of a number of factors, including the technology at issue, whether the technology can be reverse engineered, whether there is a significant question as to patent eligibility, the cost of patenting, and a number of other factors beyond the scope of this article. Last year, we presented considerations for determining whether to protect artificial intelligence technology

using patents or trade secrets. We included the chart below to capture some of the major factors one can consider in deciding between the two mechanisms:



Of course, an important issue to keep in mind is that once a trade secret is published in a patent application and/or patent, the trade secret no longer exists because it is public information, so deciding how to protect your intellectual property should be done early in the process and before anything is filed anywhere. *E.g.*, *Intellisoft, Ltd. v. Wistron Corp.*, H044281 (Cal. App. Ct. Oct. 16, 2019) (affirming judgment in favor of defendants and rejecting argument that trade secrets should still be protected despite disclosure in patent because third party published trade secret in patent, not plaintiff).

Where remote interactions are likely to continue, companies should reassess protections over their technology and sensitive information, including whether frequent and widespread remote access changes the patent v. trade secret calculus. If there is significant concern that

protocols limiting sharing of trade secrets will not be adopted, followed, and enforced as a matter of course, a company may want to consider patenting as part of its strategy (assuming eligibility) because once patented, the protection follows regardless of disclosure. That determination would need close review of all of the relevant factors; the point here is that the close review should be done. Our ways of doing business have changed considerably and possibly forever and so the questions that need to be asked: are the ways you did things pre-pandemic still sufficient now and looking ahead? And have you received any data points during the pandemic that suggest to you a change is needed – were there "close calls" that were fully addressed or is a new way of thinking about your IP protections warranted?

7. Define trade secret (or other intellectual property) ownership in any joint venture or other business arrangement

Whether negotiating and closing a joint venture or other business arrangement remotely or in-person, it is important to clearly define ownership and other rights over any intellectual property at issue, including trade secrets. For example, you do not want to find yourself in a situation where you feel like you need to act quickly to prevent the unauthorized use of a trade secret only to find out that you need signoff from another party. While all parties may be happy and look forward to the future on the day a deal closes, good relationships sour, perspectives change, risks are weighed differently, and the party who needs to sign-off on the enforcement efforts may not be willing to incur litigation costs, leaving you to make some difficult decisions. Maneuvering through that minefield, making sure the right people are connected and informed to make a decision, and having open and frank discussions about who has what rights and what steps need to be followed in light of those rights is difficult under any circumstances. Our developed proficiency in videoconferencing can make connecting over long distances easier in many respects, but the trust and mutual good faith developed from prior in-person interactions can go far in smoothing over thorny issues. If an in-person dynamic was never part of the relationship, don't expect to be able to rely on it when difficulties arise.

The better course is to prevent those difficulties in defining rights in intellectual property from ever becoming an issue by setting forth precisely in the deal documents each party's rights with respect to any intellectual property ownership, use, license, enforcement, and other rights. Make sure, for example, to define terms clearly and identify owners of any intellectual property, including any pre-existing intellectual property and any intellectual property developed during the relationship.

8. If you are in litigation, negotiate a strong protective order

To the extent litigation is necessary to protect your trade secrets, make sure there are provisions in the protective order that afford you needed protections. That could include multiple levels of confidentiality (confidential, highly confidential, and attorneys' eyes only), protocols for inspecting sensitive information, limitations on use during the litigation, and requirements for destroying sensitive information at the conclusion of the matter. Because depositions and proceedings are occurring in many matters remotely, also consider including in your protective order terms that govern how documents and information are to be handled once a remote deposition is done, who can participate in and view a deposition or other

proceeding, and how serving and filing documents under seal are to be handled while the litigation is ongoing and at the conclusion of the matter.

9. Additional Considerations

This article is not meant to be an exhaustive listing of ways to preserve or destroy a trade secret; rather, the previous sections describe some of the more common watch-outs. Other considerations to keep in mind include:

- **Factor in disclosure sensitivity and context.** Ensuring NDA terms are sufficient under the circumstances given the sensitivity of the information and context of the disclosure.
- **Apply protocols with consistency.** Being mindful that if you have aggressive confidentiality requirements, adhere to them. As noted above, picking and choosing when to follow confidentiality protocols is unlikely to be a favorably viewed if litigation ensues.
- **Know your industry.** Considering whether your industry is one in which trade secrets are particularly vulnerable (white papers, source code and software generally).
- **Keep abreast of the technology landscape.** Assessing the evolving technological landscape relative to your trade secrets as the passage of time and other industry developments may render obsolete or reduce the economic value of what was once a trade secret worthy of strong protective measures.