wgs

The Sedona Conference

Commentary on Sharing Trade Secrets with Other Organizations

A Project of The Sedona Conference
Working Group on Trade Secrets (WG12)

May 2025
Public Comment Version
Submit comments by July 1, 2025,
to comments@sedonaconference.org

The Sedona Conference Commentary on Sharing Trade Secrets with Other Organizations

A Project of The Sedona Conference Working Group (WG12) on Trade Secrets

MAY 2025 PUBLIC COMMENT VERSION

Author: The Sedona Conference

Editors-in-Chief

David Almeling Vicki Cundiff

Managing Editor

Casey Mangan

Senior Editors

Dean Pelletier Dina Hayes

Contributing Editors

John Barry Kerri Braun Jonathan Engler Jim Flynn
Astor Heaven Daniel Forester Amber Harezlak Cameron Fine
Rob Isackson Daniel Saeedi Heather Schroder

WG12 Judicial Advisor: Hon. Donald Parsons (Ret.)

Staff Editor: Craig Morgan

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

Preface

Welcome to the May 2025 Public Comment Version of The Sedona Conference's *Commentary on Sharing Trade Secrets With Other Organizations*, a project of The Sedona Conference Working Group 12 on Trade Secrets (WG12). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law.

The mission of The Sedona Conference is to move the law forward in a reasoned and just way. The mission of WG12, formed in 2018, is "to develop consensus and nonpartisan principles for managing trade secret litigation and well-vetted guidelines for consideration in protecting trade secrets, recognizing that every organization has and uses trade secrets, that trade secret disputes frequently intersect with other important public policies such as employee mobility and international trade, and that trade secret disputes are litigated in both state and federal courts." The Working Group consists of members representing all stakeholders in trade secret law and litigation.

The WG12 Brainstorming Group to develop this *Commentary* was launched in December 2021. Early drafts of this publication (including the Brainstorming Group's project charter) were a focus of dialogue at the WG12 Annual Meeting in Reston, Virginia, in September 2022, the WG12 Annual Meeting in Minneapolis, Minnesota, in September 2023, and the WG12 Annual Meeting in Phoenix, Arizona, in September 2024. The editors have reviewed the comments received through the Working Group Series review and comment process.

This *Commentary* represents the collective efforts of many individual contributors. On behalf of The Sedona Conference, I thank in particular David Almeling, the Chair of the WG12 Steering Committee, and Victoria Cundiff, now Chair Emeritus of the Steering Committee, who serve as the Editors-in-Chief of this *Commentary*, and Dina Hayes and Dean Pelletier who serve as the Senior Editors. I also thank everyone else involved for their time and attention during this extensive drafting and editing process, including our Contributing Editors John Barry, Kerri Braun, Jonathan Engler, Cameron Fine, Jim Flynn, Daniel Forester, Amber Harezlak, Astor Heaven, Rob Isackson, Daniel Saeedi, and Heather Schroder, and our Judicial Advisor, the Hon. Donald Parsons (Ret.). The drafting process for this *Commentary* has also been supported by the entire WG12 Steering Committee.

The statements in this *Commentary* are solely those of the nonjudicial members of the Working Group; they do not represent any judicial endorsement of any recommended practices.

Please note that this version of the *Commentary* is open for public comment through July 1, 2025, and suggestions for improvements are welcome. After the deadline for public comment has passed, the drafting team will review the public comments and determine what edits are appropriate for the final version. Please send comments to comments@sedonaconference.org.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG12 and several other Working Groups in the areas of artificial intelligence and the law, electronic document management and discovery, cross-border discovery and data protection law, international data transfers, data security and privacy liability, and patent litigation best practices. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be.

Kenneth J. Withers
Executive Director
The Sedona Conference
May 2025

Table of Contents

I. INTRODUCTION

Capitalizing on economic benefits of a trade secret often requires the owner to disclose the trade secret to an outsider for evaluation, use or regulatory approval. A key aspect of such disclosure, or sharing, is that the trade secret be reasonably protected under the corresponding circumstances.

Despite the recognized need to share information in the real world, little written guidance has been provided to entities that need or want to share trade secrets with another organization. In particular, there is little written guidance on protecting trade secrets before, during and after the period in which they are shared, leaving an opportunity to consider how best to approach intelligent sharing of one's valuable, secret information.

Typically, a trade secret owner will share a trade secret with another organization only in exchange for an acceptable commercial benefit. For example, such sharing might occur (1) between businesses engaging in due diligence or otherwise exploring a potential relationship or engaging in an actual relationship, such as a license, collaboration or joint venture, or (2) between a business and a regulator, where the business is seeking approval or responding to a regulatory inquiry. Each scenario simultaneously raises confidentiality concerns or risks, which initially can arise in connection with sharing the trade secrets and subsequently can arise in connection with disentangling from, winding down or terminating any due diligence, exploration or relationship. Such subsequent concerns are akin to concerns that arise in connection with employee departures.[1]

Ultimately, balancing such benefit and risk is an important consideration when exploring, engaging in and, if or when necessary, disentangling from, winding down or terminating a relationship.

A key, but not unique, risk in business-to-business sharing is trade secret status can be lost if reasonable efforts or measures to maintain secrecy are not made. What can be unique in this commercial context is how to address that risk. Overall, due to tension between disclosure and protection, sharing should take place only after the disclosing party, e.g., the trade secret owner, secures suitable and verifiable protective efforts from the receiving party. Such efforts can be specified or embodied in contractual, physical or technological tools, or a combination thereof, that define, document and control the receiving party's acquisition, access, review, disclosure, use, protection, return and destruction (collectively, processing) of the trade secrets and corresponding materials, including documents and embodiments.

This *Commentary* addresses the risk-benefit balance by focusing on protecting trade secrets before, during and after sharing, while not unreasonably hampering either party's business operations or desire to engage in due diligence or a relationship. As noted above, such protection can be achieved through contractual, physical or technological tools. In more specific terms, those tools can include

---

[1] The Sedona Conference, *Commentary on Protecting Trade Secrets Throughout the Employment Life Cycle*, 23 SEDONA CONF. J. 807 (2022), *available at* https://thesedonaconference.org/ substantively analyzes, for example, trade secret considerations that can arise in connection with employee departures.

listing and identifying the trade secrets that are shared, designating specific individuals with whom the trade secrets are or can be shared and specifying the purpose of the sharing, all of which would be part of the above-noted defining, documenting and controlling the receiving party's processing of the trade secrets and corresponding materials. This *Commentary* concludes with a helpful Appendix which provides, in list form, some helpful questions for those disclosing to and those receiving trade secrets from a third-party organization.

Importantly, any such tools and, more broadly, any trade secret sharing, whether for commercial or regulatory purposes, will create an evidentiary record that may be part of subsequent litigation or arbitration involving one or more of the shared trade secrets. Such a possibility can inform choices about which tools to employ and how to employ them, bearing in mind that the use or omission of certain tools can impact the outcome of a litigation or arbitration.

The goal of the *Commentary* is two-fold: (1) to identify potential issues when sharing trade secrets outside an organization and (2) to suggest pragmatic, potential solutions in light of marketplace reality. There is no one-size-fits-all approach for sharing trade secrets outside an organization, whether sharing trade secrets as stand-alone assets, or as assets that are part of a broader transaction. As such, the potential solutions, which are sometimes described herein as recommendations, are not intended to be and are not mandatory in any or every situation. Notably, artificial intelligence (AI) has a significant and growing role in the intellectual property arena. Regarding trade secrets, AI presents multiple opportunities and risks. An AI system, as well as one or more of its components, can be a trade secret, a tool or both. This *Commentary* addresses certain aspects of trade secret sharing where AI can be at issue in either or both capacities. As the relationship between AI and trade secrets evolves and the AI legal and regulatory landscape develops, updated or new commentary on these topics is expected. This *Commentary* does not address whether any specific tools, protections, steps, measures or combination thereof constitutes reasonable efforts to maintain the secrecy of a trade secret because such a conclusion depends on the circumstances at issue and is a question of fact to be determined by a judge, jury or other fact finder.[2] This *Commentary* also does not address any domestic or foreign data privacy laws or regulations or how they might impact trade secret sharing within the United States or between the United States and a foreign country.

---

[2] References in this *Commentary* to a "trade secret" are not meant to imply that a court or other authority, such as the U.S. International Trade Commission or an arbitrator, has concluded that the information is, in fact, a trade secret. Instead, a reference to a "trade secret" is a reference to an alleged or asserted trade secret. For more details regarding identification of trade secrets issues, *see* The Sedona Conference, *Commentary on the Proper Identification of Asserted Trade Secrets in Misappropriation Cases,* 22 SEDONA CONF. J. 223 (2021).

II. REASONS FOR SHARING TRADE SECRETS WITH OTHER ORGANIZATIONS

Due diligence that includes sharing trade secrets typically involves uniquely situated parties and correspondingly unique challenges and risks. More specifically, the disclosing party and receiving party typically are organized differently and possess different types and amounts of resources. Their methods of operations, cultures, policies, procedures and levels of expertise with trade secrets and, on a higher level, with contract and information management also can vary. Such circumstances require deliberate discussion and, ultimately, tailored approaches to maintain the confidentiality of shared trade secrets.

In addition to each party's respective make-up, the contemplated and ultimate form of the parties' relationship informs the parties' approach during due diligence and beyond. For example, a joint venture or joint development work may require greater diligence before entering a formal relationship and more detailed, ongoing assessments of trade secret disclosure and use during the relationship than is typically required in connection with a narrower relationship, such as an investment in a start-up or a supply agreement. Further, if information, including trade secrets, is to be shared between competitors or potential competitors, then potential applicability of antitrust laws may need to be considered and certain guardrails, such as clean rooms, may need to be implemented to mitigate or avoid contamination or inappropriate sharing that might violate or lead to violation of those laws.[3]

The nature of a trade secret to be shared, including its value and form, also may inform the parties' discussion regarding an approach to protecting the trade secret. For example, the value of the trade secret to the disclosing party can, and often does, result in proportional levels of diligence and safeguards for that asset. As another example, where the trade secret is a single, i.e., the only, prototype, the receiving party's access to the asset can and often will be in-person, site-specific and monitored.

Further, the parties often face time constraints. In other words, the parties may wish or need to quickly evaluate a potential business opportunity involving trade secrets. Such circumstances require balancing the time constraints with the need to protect the trade secrets. Trade secret owners who know what their trade secrets are and how they protect them are positioned to nimbly achieve that balance.

As to solutions, a confidentiality or non-disclosure agreement (NDA) is an example of a common tool used to protect trade secrets. Importantly, the rights, limitations and obligations set forth in an NDA, and in any broader agreement governing the parties' relationship, and the selection and

---

[3] For additional guidance about clean rooms, *see* The Sedona Conference, *Commentary on the Use of Clean Rooms*, *Public Comment Version* (March 2025), *available at* https://thesedonaconference.org/publication/Commentary_on_Use_of_Clean_Rooms.

tailoring of other tools used to protect trade secrets can be impacted by multiple factors.[4] Such factors include the parties' respective makeup, as noted above, the contemplated or ultimate form of the parties' relationship, the specific trade secrets at issue, the parties' past dealings with each other and their respective existing or potential third-party relationships, including a future merger, acquisition or sale of a party's business. Where the parties' overall relationship is defined in a written agreement broader than an NDA, such an agreement can set forth how, why, when, where and with whom trade secrets can be shared, and a protocol if the status, such as control, of either party changes during the term of such agreement. The agreement also may indicate what the trade secrets are by setting forth categories, or types or general subject matter, of information. Setting forth categories of information does not mean identifying the trade secrets in the agreement. Rather, and for example, the agreement can cross-reference a securely stored addendum identifying or a secure depository for the trade secrets.[5]

Some common forms of relationships or contexts in which trade secrets may be shared include:

License: Generally speaking, a license is an agreement where the owner of certain subject matter, such as a trade secret, grants another individual or entity certain rights, such as the rights to access, disclose and use the trade secret.[6] Notably, the owner, i.e., licensor, retains ownership of, and corresponding rights to and interests in, the licensed subject matter, despite the grant of rights to the authorized party, i.e., licensee.

Licenses come in all shapes and sizes. They include various limitations, i.e., conditions or qualifications, such as: the duration of the license, bearing in mind that a license may be renewable and typically can be terminated, and that certain obligations, such as confidentiality obligations, may continue after a license expires or is terminated; authorization to use a trade secret for only a specific or limited purpose, such as to design, develop or sell a certain product or service, for only personal or commercial use or for use only in a specific field, market or geographic area; and the status of a licensee, such as a single, or exclusive, licensee or exclusivity in a certain product, service, field, market or geographical area.

Supply Relationship: In a supply relationship, a supplier, such as a vendor or independent contractor, provides goods, such as inputs, or services, such as fabrication of inputs, to a customer. Those

---

4 An NDA can be a stand-alone agreement, or it can be a portion of or provision within a broader agreement. For additional guidance about NDAs, *see* The Sedona Conference, *Commentary on Protecting Trade Secrets Throughout The Employment Life Cycle*, 23 SEDONA CONFERENCE J. 807 (2022).

5 Setting forth categories of information, as opposed to identifying trade secrets at issue, is an example of implementing the "need-to-know" practice to protect trade secrets. In other words, certain persons in the receiving party's operations who are responsible for business functions, including contract negotiation and management, may not need to know what the trade secrets are to fulfill their responsibilities.

6 *See* Defend Trade Secrets Act (DTSA), 18 U.S.C. § 1839(4) ("the term 'owner', with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed").

goods or services may embody or have been produced with a trade secret—owned by the supplier or customer. Alternatively or additionally, a trade secret may be provided with a product or service to enable implementation or ensure compatibility with another product or service. These agreements are common in many industries and can play a major role in the functioning of national and global supply chains.

Supply agreements often include clauses addressing quantity, quality, product or service specifications, delivery time, cost of transportation and other parameters. Such a clause may constitute or include a trade secret. Additionally, where a supply agreement is part of or evolves into a longer term or ongoing relationship, the parties may enter a master service agreement (MSA). An MSA can include baseline provisions, including, for example, a baseline confidentiality provision, applicable to all or certain aspects of products and services.

Joint Venture, Joint Development or Other Collaboration: In some cases, a single company or individual may lack the expertise or resources to develop or bring to market a product or service. In these circumstances, two or more parties may enter a business arrangement establishing a joint commercial enterprise where each party takes on specific responsibilities and corresponding costs and risks, and profits are apportioned. This type of arrangement is commonly referred to as a joint venture.

Joint ventures are common in many industries, such as the life sciences and pharmaceutical industries, and often involve research and development. For example, a company that has researched and developed science and technology around a device, diagnostic test or treatment may lack resources such as financial, human or manufacturing capital, capabilities, or expertise to seek and obtain regulatory approval for, or to develop, market and sell the device, test or treatment. That company may then form a joint venture with another company that can provide the necessary resources. Trade secrets may be shared and, in some situations, created as part of those joint efforts. Some or all of those trade secrets may constitute a capital contribution to the joint venture.

Sale of Goods or Services: A sale of goods or services is a basic and common transaction where one party, a seller, contracts with another party, a buyer, to transfer ownership of goods or render services in exchange for consideration. A supply relationship, which is discussed above, and a sale are separately mentioned because a supply relationship often involves providing inputs and a sale often involves providing the final or finished good or service.

Merger, Acquisition or Sale of All or Substantially All Assets: Mergers, acquisitions and sales of assets typically are transformative transactions. In a merger, one entity combines with another entity to create a new, singular entity. The new entity acquires all assets and liabilities of the absorbed entity. In an acquisition, one entity takes over another entity by purchasing all or most of the target entity's shares or other equity interests. In a sale of all, substantially all or certain assets, one entity purchases specified assets and liabilities of a target entity.

Each type of transaction can present unique trade secret sharing issues. For context, each type of transaction may involve a transfer of trade secrets between the parties to the transaction or a

continuation of, or a need to modify, previous or existing trade secret sharing between those parties or between a party to the transaction and a third party.

Notably, the ultimate consummation of such a transaction may not present the most significant, or any, trade secret sharing risks. Rather, due diligence preceding the transaction may present such risks. That is, depending on the particular transaction contemplated, a seller may share trade secrets with multiple prospective buyers. Such sharing needs to be handled carefully to ensure trade secret status is intact when only one buyer remains.

Investment, Including Securitization for Debt Financing: An entity or individual may acquire an interest in another entity in exchange for financial or another type of support. For example, a startup company may lack financial capital to develop, market or sell a product and, as a result, seek financing and possibly other capital, including human capital or expertise, from investors.

A common source of capital for founders of a startup who wish to retain an ownership interest in their company is venture capital (VC), private equity (PE) or both. In a typical investment model, a VC or PE firm will assess that opportunity through due diligence that includes evaluation of the startup's operations and assets, including trade secrets and other intellectual property (IP).[7] If satisfied with that assessment, the firm may invest financial capital into the startup in exchange for an ownership interest in the startup. That is, the founders may sell all or part of their interests in the startup to the firm. The firm often gains a seat on or control of the startup's board of directors and, beyond the capital contribution, provides expertise to assist with the management and growth of the startup and commercialization of the startup's products or services.[8]

In another perhaps less common scenario, a startup may seek an infusion of financial capital though debt financing where it seeks to secure or collateralize the loan through certain assets, such as trade secrets. In such an arrangement, the trade secrets may be shared with the lender so the lender can perform its due diligence on, for example, the claimed status, i.e., confidentiality, and value of the pledged collateral.

Regulatory Approval: Advertising, marketing, selling or otherwise providing certain products or services to the public is regulated on many levels, ranging from international, national, state to local levels.

In the United States, regulators at the national level include the Department of Transportation (DOT), the Food and Drug Administration (FDA), the Occupational Safety and Health

---

[7] Trade secrets are not identified in any governmental grant or registration like patents, trademarks and copyrights are. Because of that lack of official documentation, evaluation of trade secrets often requires greater effort than evaluation of other IP. This *Commentary* is designed, in part, to facilitate that greater effort and, ultimately, sufficient evaluation of the trade secrets at issue.

[8] Where a PE firm invests financial capital after a VC firm, the PE investment may replace or offset the VC investment.

Administration (OSHA) and the Environmental Protection Agency (EPA). Assuming federal regulatory approval has been obtained for a product, service or facility, there also may be a need for state or local regulatory approval, such as with compounding pharmacies.[9]

While each regulator has its own specific process for applicants seeking and obtaining approval, a typical component of such a process is submission of sufficiently detailed information about the product or service at issue. Those submissions often are written. In certain circumstances, information also may be provided through an on-site inspection of a facility or operations. Such information can include, for example, safety and efficacy data from clinical or other trials or safety of a facility or operations. Notably, such information can include one or more trade secrets. Such inclusion is important because any information submitted or provided is at risk of public disclosure through the regulator's response to a Freedom of Information Act (FOIA), 5 U.S.C. § 552, request, a similar mechanism or otherwise. Indeed, that risk exists despite potential penalties for officers and employees of the United States and U.S. departments and agencies, such as the U.S. Department of Justice and Federal Trade Commission (FTC), who wrongfully disclose trade secrets.[10]

Additionally, existing and proposed laws and regulations impose or may impose record-keeping and disclosure obligations on developers and deployers of artificial intelligence (AI) systems. Such obligations can encompass, for example, technical information, such as training, testing and evaluation

---

9 Pursuant to section 503A of the Federal Food, Drug, and Cosmetic Act (FDCA), compounding pharmacies are allowed to provide drug products for patients whose clinical needs cannot be met by an FDA-approved drug product. Such pharmacies are exempt from certain sections of the FDCA, but only if the pharmacy is a State-licensed pharmacy. *See* U.S.C. §503A (exempting State-licensed pharmacies from § 501(a)(2)(B), which addresses current good manufacturing practice requirements, § 502(f)(1), which addresses labeling drugs with adequate directions for use, and § 505, which addresses approving drugs under new drug applications or abbreviated new drug applications). *See also* the Federal Trade Commission Act, 15 U.S.C. § 46(f) (addressing whether commercial or financial information obtained by the Federal Trade Commission can be maintained as confidential or privileged) *and* the Antitrust Civil Process Act, 15 U.S.C. §§ 1311-1314 (addressing potential exclusion of a Freedom of Information Act (FOIA), 5 U.S.C. § 552, request).

10 *See* 18 U.S.C. § 1905 ("Whoever, being an officer or employee of the United States or of any department or agency thereof, any person acting on behalf of the Federal Housing Finance Agency, or agent of the Department of Justice . . . , or being an employee of a private sector organization who is or was assigned to an agency . . ., publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties or by reason of any examination or investigation made by, or return, report or record made to or filed with, such department or agency or officer or employee thereof, which information concerns or relates to the trade secrets . . . of any person, firm, partnership, corporation, or association; shall be fined under this title, or imprisoned not more than one year, or both; and shall be removed from office or employment.") and FOIA Exemption 4; *see also* 20 CFR § 402.90; and see, *e.g.*, Department of Justice Releases New Guidance on FOIA Exemption 4, The FOIA Ombudsman, available at https://foia.blogs.archives.gov/2019/10/21/department-of-justice-releases-new-guidance-on-foia-exemption-4/. For an example at the state level, see, *e.g.*, N.J.S.A. 47:1A-1.1, Government Records Exemption No. 6 ("Trade secrets and proprietary commercial or financial information obtained from any source. For the purposes of this paragraph, trade secrets shall include data processing software obtained by a public body under a licensing agreement which prohibits its disclosure"), available at https://www.nj.gov/dep/opra/exemptions.html.

data, processes and results, as well as risks and realized harms, such as discrimination.[11] Such obligations seek to achieve, for example, transparency, traceability and explainability for AI regulators, deployers and end users.[12] Importantly, trade secrets and other information may be excluded from disclosure obligations.[13] Whether or not such an exclusion applies, a receiving party may be obligated to maintain the confidentiality of disclosed trade secrets and other information.[14] In practice, the levels of record-keeping and disclosure required or deemed sufficient may vary by jurisdiction, i.e., by applicable legal and regulatory frameworks, and the particular circumstances at issue and likely will evolve over time. For a trade secret owner, a key takeaway or reminder is that the trade secret or confidential status of disclosed information can be eliminated or put at risk through disclosure. So, an informed and incremental approach to disclosure, especially with new and developing frameworks, can be a sound approach.

In some situations, persons subject to such laws and regulations will want to avoid needlessly eliminating or risking trade-secret status through excessive disclosure. So, a trade secret owner or holder may need or want to seek guidance or clarification from the corresponding regulator or other authority before or in connection with making any disclosure.[15]

---

11 *See, e.g.,* EU AI Act, Art. 53(1)(a) *and* Colorado (CO) AI Act, SB 24–205 §§ 6-1-1702-1704.

12 *See, e.g., id. and* EU AI Act, Recital 27 ("Transparency means that AI systems are developed and used in a way that allows appropriate traceability and explainability, while making humans aware that they communicate or interact with an AI system, as well as duly informing deployers of the capabilities and limitations of that AI system and affected persons about their rights.")

13 CO AI Act, SB 24–205 §§ 6-1-1702(6), 6-1-1703(8).

14 *See, e.g.,* EU AI Act, Art. 53(7) and 78. *See also* note 8, *supra* (noting 18 U.S.C. § 1905).

15 Other situations where there may be a reason to share trade secrets with another organization include litigation finance and trade secret insurance transactions.

III. TOOLS AVAILABLE WHEN SHARING TRADE SECRETS

Parties who share trade secrets often proceed through a sequence of (1) pre-sharing, (2) sharing and (3) post-sharing. In other words, the sequence has three general periods: (1) the pre-due diligence or pre-relationship period (collectively, pre-sharing), (2) the due diligence or relationship period, (3) the post-due diligence or post-relationship period. Of course, due diligence may or may not result in a relationship and there may be a disentanglement or wind down before termination of the parties' interactions and commencement of the post-due diligence or post-relationship period.

Parties in a pre-sharing period may want to and perhaps should engage in high-level, exploratory discussions to determine whether deeper discussions, including sharing trade secrets, should proceed. Those exploratory discussions can focus on big-picture issues, such as contemplated forms of a relationship and the role of trade secrets in deeper discussions or a relationship. In turn, exploratory discussions may reveal obstacles that make actual due diligence or a relationship and initial or further trade secret sharing impractical or unappealing for commercial or other reasons. Notably, individuals engaging in exploratory discussions may not be and, in some cases, intentionally should not be the same individuals who will access, review and use shared trade secrets during due diligence or a relationship. In short, exploratory discussions can allow parties to walk away from a potential due diligence or relationship without having shared any trade secrets, or having shared only a high-level, non-confidential description of trade secrets, a representative trade secret or a limited number of trade secrets, thereby reducing, and perhaps eliminating, the risk of a subsequent trade-secret dispute and related consequences.

If or when the parties decide to proceed with deeper discussions or to engage in due diligence or a relationship, there are three major categories of protective measures that a disclosing party may use to protect its trade secrets before, when and after the trade secrets are shared: (1) contractual tools, (2) physical tools, and (3) technological tools. Contractual tools, which are key administrative tools, can include NDAs and other agreements with confidentiality obligations, such as clean room or clean team agreements. Physical tools can include clean rooms for accessing and reviewing trade secrets.[16] Technological tools can include passwords and multi-factor authentication that restrict access to electronically or digitally stored trade secrets and enable monitoring of such access. Notably, training personnel is an overarching administrative tool that can be used to implement and bolster contractual, physical and technological tools. Indeed, training can foster a culture where trade-secret policies and procedures are understood and followed. Each category is further discussed below.[17]

---

16 For additional guidance about clean rooms, *see* The Sedona Conference, *Commentary on the Use of Clean Rooms*, *Public Comment Version* (March 2025), *available at* https://thesedonaconference.org/publication/Commentary_on_Use_of_Clean_Rooms.

17 *See* SBS Worldwide, Inc. v. Potts, No. 13 C 6557, 2014 WL 499001, at *5 (N.D. Ill. Feb. 7, 2014) (plaintiff/ disclosing party adequately alleged it took reasonable measures to protect its trade secrets with a mixture of contractual, physical and technological tools).

Principle No. 1: Before and when trade secrets are shared, contractual tools, physical tools and technological tools can be used to protect the trade secrets and those tools can be supplemented, modified or enhanced throughout due diligence or a relationship.

IV. CONSIDERATIONS BEFORE DUE DILIGENCE OR A RELATIONSHIP

A. Personnel Involved

Principle No. 2: Sharing trade secrets calls for respective vigilance by designated personnel, such as a trade secret team, which may include a manager responsible for overseeing trade secret sharing, one or more individuals responsible for a certain aspect of that sharing, and in-house or outside counsel.

For a disclosing party, a starting point for sharing trade secrets with another organization can be assembling a team of individuals who will be engaged in sharing and protecting the trade secrets (Team). The Team members may be employees, agents or other representatives of the disclosing party. An in-house or outside counsel may be a Team member. The Team can focus on, for example, identification of the categories of information to be shared, the trade secrets to be shared, the selection and implementation of measures to protect the trade secrets and active monitoring of the receiving party's activities and compliance with its obligations.

Each Team member can be responsible for a specific area. Those areas can include: (1) project management, including communication and coordination with the receiving party, (2) subject matter expertise, i.e., knowledge of the trade secrets and any related information, to determine what can be shared or not, (3) legal expertise to identify the trade secrets and rights in and authorization to share the trade secrets, (4) security, including physical or facility security, (5) data governance to account for applicable data policies and procedures, (6) information technology, including data management, to coordinate secure, electronic storage of and access to the trade secrets, (7) compliance, including the disclosing party's adherence to trade secret sharing protocols and the receiving party's implementation of protective measures, and (8) human resources to account for company policies and procedures relating to trade secrets. Each due diligence or relationship involving trade secret sharing is different, so a Team may include one or more of the foregoing or other individuals. For a small company, a Team may consist of only one individual or a few individuals responsible for fulfilling designated responsibilities. The volume and nature of the trade secrets, as well as the resources of a company, can also affect a Team's make-up. Where feasible, the Team should not comprise only lawyers. Non-lawyer Team members can provide unique, needed perspective and guidance during the sharing.

A receiving party can assemble its Team by accounting for the same or similar issues as the disclosing party, albeit from the opposite perspective. For example, one or more receiving party Team members presumably possess relevant, sufficient subject matter knowledge to assess the shared trade secrets and contemplated opportunity. Having said that, the receiving party may intentionally exclude from its Team one or more individuals who are integral to its operations. Such exclusion can avoid exposing those individuals to trade secrets and, as such, sufficiently preserve the receiving party's ability to continue, re-engage in or initiate its own pursuits if or when, for example, the parties' interactions end or due diligence terminates. To facilitate such exclusion and related efforts, such as clean room management, the receiving party can internally identify its current or planned

pursuits that sufficiently relate or may relate to the trade secrets. Overall, a receiving party Team will focus on complying with applicable obligations, preventing missteps, such as inadvertently commingling disclosing party trade secrets with receiving party trade secrets or other information, and avoiding disputes relating to disclosing party trade secrets.

Notably, a disclosing party may request or require that a receiving party Team not include any individual who has worked with, is working with or is expected to work with any existing or contemplated competing technology or subject matter, including any in-house or outside patent attorney or agent.[18] Such an exclusion can benefit both the disclosing party and receiving party by reducing the risk of a trade-secret misappropriation, breach of contract or other dispute.

Having said that, a receiving party may believe an exclusion will unduly inhibit its analysis and either (1) not agree to a requested or required exclusion or (2) seek a narrower exclusion, such as an exclusion of any individual who has researched or developed, is researching or developing or is expected to research or develop any existing or contemplated competing technology or subject matter. Before taking either of those positions, the receiving party should consider that an exclusion, and even a relatively broad exclusion, can be advantageous from an operational perspective. More specifically, an exclusion can avoid contamination of the receiving party's operations such that, if the parties' interaction is terminated, the receiving party can proceed with greater confidence that its pursuits will be uninterrupted by concerns of or actions by the disclosing party.

Where such an exclusion is not implemented, and the disclosing party is still willing to share its trade secrets, then modifications to the sharing process may be an option.[19] For example, the trade secrets may be shared in (a) sequenced fashion, i.e., trade secrets are gradually shared as opposed to all at once, or (b) segmented fashion, i.e., a part or parts of trade secrets are shared and then the complete trade secrets are shared if the parties decide to proceed with due diligence or a relationship.

If the disclosing party and receiving party are actual or potential competitors, then a data room, which may be or include a clean room, is an option to consider. Data rooms are further discussed below.

Team members should be contractually bound to protect any trade secrets disclosed or received. At least for the disclosing party Team, such contracts may exist prior to any sharing. If such a contract does not exist prior to any sharing, then the benefits of becoming a Team member may constitute sufficient consideration for a new or supplemented contractual obligation. A designated Team member or members can be responsible for ensuring proper contracts are in place and ensuring

---

[18] *See* Wellogix, Inc. v. Accenture, LLP*,* 823 F. Supp. 2d 555, 566 (S.D. Tex. 2011) (affirming jury's finding that the receiving party in a sharing relationship received trade secrets and was liable for trade secret misappropriation where it used this information in subsequent work for third parties), *aff'd sub nom.* Wellogix, Inc. v. Accenture, L.L.P., 716 F.3d 867 (5th Cir. 2013).

[19] In some situations, an exclusion may not be implemented because it is not feasible. A lack of feasibility may exist, for example, where a receiving party is a relatively small company with a correspondingly small group of employees.

compliance with the contracts as a whole or with specific provisions, such as return or destruction of trade secrets. By obtaining copies of such executed contracts, the disclosing party can verify the receiving party has such contracts in place and confirm the roster of authorized individuals. The use of such contracts, or supplementation of existing contracts, in connection with the sharing is further discussed below.

Finally, some employers periodically train, or at least remind employees about the value of and obligations to protect trade secrets. Such efforts can account for applicable NDAs and other agreements. Similarly, the disclosing party and receiving party can agree to train or remind Team members and others involved in the trade secret sharing about their obligations relating to trade secrets in general and the trade secrets to be shared. The frequency and extent of such training or reminding can be affected by the duration of the parties' interaction, due diligence or relationship.

B. Assets At Issue

Principle No. 3: Trade secret sharing can be gradual, such that before trade secrets are shared, the parties can agree in writing on the types of trade secrets, by category, intended to be shared, and any such categories can be specific enough to make clear the types of information the receiving party will be obligated to protect.

1. Identification of Trade Secrets to Be Shared

Before any trade secrets are shared, the disclosing party can determine, perhaps in collaboration with the receiving party, the categories of information that the disclosing party will share and that the receiving party will need to evaluate or effectuate the potential or actual relationship. Designating and, if necessary, updating those categories can ensure that the disclosing party focuses its efforts and limits its disclosure and risks and that the receiving party likewise limits its risks. Disclosing no more than necessary and receiving no more than necessary are mutually compatible goals.

A disclosing party may be balancing two concerns when providing categories of information to the receiving party. On the one hand, categories should not be so detailed or specific that they reveal any trade secret. That is, absent appropriate protections, providing overly detailed categories can jeopardize trade-secret status. On the other hand, categories that are too general may not provide the receiving party with an ability to sufficiently understand the actual or potential relationship, the relevance of the information already in its possession, which information may establish that a claimed trade secret is already known to it, or the expectations for or scope of protective measures.

In some cases, both the disclosing party and receiving party will know the categories of the information to be shared at the outset of their interactions. In other cases, there may be a need for collaboration between the parties following a high-level, initial disclosure. Ultimately, the disclosing party should describe the categories of information to be shared with enough specificity to make clear the

types of information the receiving party will be obligated to protect throughout the due diligence or relationship so that proper safeguards can be agreed to and implemented.

A subsequent step for the disclosing party is to gather the information in those categories that will be shared. Within those categories, information may be (1) a trade secret, (2) confidential, sensitive or proprietary information that does not satisfy the legal definition of a trade secret or (3) publicly or generally known information. A disclosing party's appreciation for, and proper accounting of, those different types of information is or can become important from an overall information governance or contract (e.g., license) management perspective, including where, as noted above, trade secrets and other information are submitted to a regulatory authority and non-trade-secret information is later sought through, for example, a FOIA request. Additionally, if information is publicly or generally known, then a disclosing party can share that information without protection and, as a result, potentially save time, money, and effort.

Once collected, a disclosing party should separate its trade secrets from the non-trade secret information so that the trade secrets can be readily tracked and, at the appropriate time, properly shared. Notably, this sharing may occur all at once, gradually or in stages. Such an approach can benefit both parties. A disclosing party that discloses fewer trade secrets, i.e., discloses only trade secrets needed to further the due diligence or other activity, exposes fewer trade secrets to risk of misappropriation or loss and can reduce expenditures of time, money and effort relating to, for example, protective tools. A receiving party that receives fewer trade secrets, i.e., receives only trade secrets needed to further the due diligence or other activity, reduces its liability exposure and likewise can reduce expenditures of time, money and effort relating to, for example, protective tools.

At this point, the disclosing party should: (1) know the categories of trade secrets that may be shared and (2) be able to identify, and should internally identify, the trade secrets that may be shared.[20]

A trade secret that is identified is set forth with sufficient particularity.[21] A prior *Commentary* addresses proper trade-secret identification in litigation and the principles and guidance in that

---

[20] *See* Walmart Inc. v. Cuker Interactive, LLC, 2020 U.S. App. LEXIS 4289, **10–12 (8th Cir. Feb. 12, 2020) (a company's failure to clearly identify an alleged trade secret before its disclosure to a client precludes trade secret status); Health Care Facilities Partners, LLC v. Diamond, No. 5:21-CV-1070, 2023 WL 3847289, at *15 (N.D. Ohio June 5, 2023) (granting summary judgment in favor of defendant where, among other reasons, the disclosing party failed to identify its shared trade secrets during the relationship and to sufficiently protect them); and Scentsational Technologies, LLC v. Pepsico, Inc., 13-cv-8645 (KBF), 2018 WL 2465370 (S.D.N.Y. May 23, 2018), *aff'd* 777 Fed. Appx 607 (FED. CIR. 2019) (trade secret claim fails without contemporaneous records describing the trade secret; such records were necessary to corroborate claim of joint creation of the trade secret).

[21] A properly identified trade secret is a trade secret identified with sufficient particularity, and the identified trade secret is distinct from the categories of information eligible for trade secret status. *See, e.g.,* DTSA, 18 U.S.C. § 1839(3) (a "trade secret" is "all forms and types of financial, business, scientific, technical, economic, or engineering information," regardless of the medium of storage, compilation or memorialization if "(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information[.]"); *and* Uniform

Commentary readily can be applied to trade secret identification in connection with due diligence or a relationship.[22] However, the context of due diligence or a relationship is different from the adversarial context of litigation. As such, the parties involved in due diligence or a relationship may agree to a less rigorous standard of sufficient particularity than would be required in misappropriation litigation.

Once the disclosing party knows the categories of trade secrets and trade secrets that may be shared, it should account for its policies and procedures for identifying and protecting trade secrets, any applicable written agreements, such as NDAs, that protect trade secrets, any other contractual, physical or technological protective measures, or tools, such as marking, secure storage, segregation, limitations on acquisition, access, disclosure and use and any monitoring of the foregoing.[23] Where a disclosing party knows how it protects its trade secrets, it will be better able to determine and require appropriate, though perhaps not identical to its own, protective measures by a receiving party during due diligence or a relationship. Ultimately, protective measures taken by the disclosing party and the receiving party, respectively and collectively, need to satisfy the legal standard of reasonable measures.[24]

Whether the protective measures taken in a situation will satisfy the reasonable measures standard is a question of fact decided on the totality of the circumstances, which may include standards

---

Trade Secrets Act (UTSA), §1(4) (""Trade secret' means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."). The UTSA or a version thereof has been adopted by 49 States, and by the District of Columbia, with the only exception being New York.

22 *See footnote 2*, *supra*, referencing The Sedona Conference, *Commentary on the Proper Identification of Asserted Trade Secrets in Misappropriation Cases,* 22 SEDONA CONF. J. 223 (2021).

23 Examples of other contractual tools may include, to the extent enforceable, noncompete and non-solicit agreements.

24 *See* DTSA, 18 U.S.C. § 1839(3) *and* UTSA, § 1(4). Importantly, the reasonable protective measures requirement accounts for measures taken by a disclosing party, as well as measures taken by a receiving party. Geritrex Corp. v. Dermarite Indus*., LLC*, 910 F. Supp. 955, 961 (S.D.N.Y. 1996) ("Plaintiff must show that it took substantial measures to protect the secret nature of its information."); Big Vision Priv. Ltd. v. E.I. DuPont de Nemours & Co., 1 F. Supp. 3d 224, 267–69 (S.D.N.Y. 2014) ("There is virtually no contemporaneous documentary or testimonial evidence . . . indicating that Big Vision took *any steps* to ensure the confidentiality of the information it disclosed to third parties."); KT Grp. Ltd. v. NCR Corp., 2018 WL 11213091, at *13 (S.D.N.Y. Sept. 29, 2018) (citing Sw. Stainless, LP v. Sappington, 582 F.3d 1176, 1190 (10th Cir. 2009)) ("[D]isclosure of the alleged trade secrets to individuals or entities who are under no obligation to protect the confidentiality of the information extinguishes the owner's property right in the purported trade secrets."); *and* Nova Chems., Inc. v. Sekisui Plastics Co., 579 F.3d 319, 327–28 (3rd Cir. 2009) (holding that information disclosed to defendant distributor pursuant to a license "lost its trade secret status" because the license agreement did not require defendant to "maintain the secrecy of any information it had acquired from [plaintiff]").

applicable in the relevant industry, the value or importance of the particular trade secret at issue and the respective sizes and resources of the disclosing and receiving parties. [25]

Beyond satisfying the legal standard is marketplace reality. That is, a disclosing party may know, based on its own efforts, what physical and technological tools are effective. A disclosing party armed with that knowledge often wants a receiving party to implement the same, or substantially or sufficiently the same, tools as the disclosing party knows to be effective. Indeed, a difference between a disclosing party's tools and the receiving party's corresponding tools may make proving the existence of reasonable protective measures more difficult and may create exploitable or exploited risks that, in fact, lead to the misappropriation of the trade secret, corresponding operational and litigation expenses and corresponding injuries, including financial losses that may not be recoverable as part of any damages award.

2. Identification of What Is Not Part of Trade Secrets to Be Shared

Before any trade secrets are shared, the disclosing party also can identify information it will not share with the receiving party in connection with the evaluation or effectuation of the potential or actual relationship. The disclosing party simply may identify and not disclose certain information on its own. Alternatively, the disclosing party and receiving party may collaboratively determine the categories of information that the disclosing party will not share with the receiving party. A contract provision authorizing a receiving party to reject receipt of information can also be employed. Such a provision can promote transparency in the information shared, encourage the receiving party to review the information shared, and limit or eliminate risks relating to information that the receiving party does not accept and, as required, returns or destroys. A contract provision authorizing the disclosing party to retrieve or claw back shared information likewise can be employed. In practice, such identification and determination and exercising of contractual provisions can avoid or enable correction of errors, such as inadvertent or excessive disclosure of information to the receiving party. But importantly, those steps are supplemental to a disclosing party monitoring the information it shares.

3. A Protocol for Potentially Sharing Additional Trade Secrets

As the evaluation or effectuation of the parties' potential or actual relationship unfolds, a need for the disclosing party to share additional trade secrets may develop. Alternatively or additionally, a need for the receiving party to share trade secrets may develop. Given those possibilities, the parties can agree to the circumstances and conditions under which the disclosing party can disclose additional trade secrets and under which the receiving party can become a disclosing party. While the terms of the parties' agreement may sufficiently account for such sharing, or certain aspects of such sharing, a substantive change to the evaluation or effectuation of the parties' potential or actual relationship, including any change in the scope of trade secret sharing or to a party's respective role as a

---

[25] *See* The Sedona Conference, *Commentary on the Governance and Management of Trade Secrets*, 24 SEDONA CONF. J. 429 (2023).

disclosing or receiving party, can lead to circumstances that warrant a review of and, as needed, revisions to the parties' existing agreement.

C. Protective Measures Before Sharing Trade Secrets

Principle No. 4: Where a party intends to share trade secrets with a receiving party, it can require the receiving party to implement initial protective measures, which are designed to be reasonable under the circumstances, before any trade secret is shared.

Sharing trade secrets with third parties increases the risk of, among other things, (1) misappropriation, i.e., unauthorized acquisition, disclosure or use of the trade secrets, and (2) loss of secrecy and, as such, loss of trade-secret status. An effective way to mitigate those risks is to implement protective measures before any trade secrets are shared and to be ready to timely enhance protective measures if sharing actually occurs.

As noted above, the three major categories of measures that a disclosing party may use to protect its trade secrets before, when and after the trade secrets are shared are: (1) contractual tools, (2) physical tools and (3) technological tools. Notably, there is no one-size-fits-all approach to protective measures. Rather, those measures must be reasonable under the circumstances to establish and maintain trade secret status. Notably, establishing reasonable protective measures does not require implementing all the specific examples of protective measures discussed below. Moreover, none of the measures, alone or in any combination, are intended to reflect, establish or suggest any standard or industry practice at any stage of a trade secret sharing process.

1. Contractual Tools

A contract often is the starting point for protecting trade secrets before sharing them.

More specifically, parties contemplating trade secret sharing often enter into a confidentiality agreement, or NDA, that governs the acquisition, access, disclosure and use of the trade secrets and imposes additional protective measures, such as physical and technological tools, for the trade secrets.[26]

---

[26] In practice, there may be differences between a confidentiality agreement and an NDA. However, in this *Commentary*, we treat the terms, i.e., agreements, as synonymous. An executed NDA often is the culmination of a drafting and negotiating process. The process typically commences when the disclosing party sends an NDA to the receiving party, with the hope that the receiving party simply will sign and return the NDA. That may happen where the disclosing party possesses greater bargaining power, including greater resources. A more typical scenario, however, especially between two similarly situated entities, is an NDA is executed after an exchange of revised drafts and negotiations. We raise this dynamic to illustrate there is no universally used NDA and, overall, each due diligence and relationship is unique. Accordingly, this *Commentary* is not meant to provide and does not provide a one-size-fits-all suggestion, recommendation, or requirement for an NDA or anything else.

An NDA typically serves several important purposes. First, an NDA provides the receiving party with notice of the categories of information into which the disclosing party's trade secrets fall. Second, an NDA establishes the receiving party's contractual obligations to maintain the secrecy, or confidentiality, of the trade secrets and to refrain from acquiring, accessing, reviewing, disclosing or using the trade secrets in a manner not authorized by, or that exceeds the authorization provided in, the NDA.[27] Third, an NDA provides remedies to the disclosing party if the receiving party breaches a contractual obligation. Fourth, an NDA is simultaneously an important protective measure and tangible evidence of reasonable protective measures, which must be taken for information to have trade-secret status.[28] Indeed, the absence of a written NDA when sharing a trade secret can make proving the existence of the trade secret, i.e., that reasonable measures were taken to protect the information at issue, more challenging and, ultimately, may eliminate a claim and remedies for trade-secret misappropriation.[29]

An NDA is also like any other contract insofar as it may not address every issue that arises. For this reason, clear communication between the parties when negotiating an NDA is important. If documented and clear, communications between the parties may facilitate resolution of an issue relating to the NDA. Also, depending on the existence, validity and enforceability of an integration clause, those communications may be evidence in litigation or an alternative dispute resolution (ADR) process.[30]

Notably, an NDA can impact and be impacted by existing and future agreements, relationships and litigation involving the parties to the NDA or involving one or more of the parties to the NDA plus one or more third parties or former employees. As such, drafting, negotiating and complying with the NDA can involve each party accounting for and coordinating existing and anticipated obligations beyond the NDA. Such accounting and coordinating ideally takes place before the NDA is

---

[27] If a dispute between the parties subsequently arises and litigation ensues, there may be an ancillary dispute over the terms of a corresponding protective order. In particular, the parties may disagree over which, if any, individuals, other than outside counsel and retained, independent experts, are authorized to acquire, access, review, disclose or use asserted trade secrets or other confidential documents and information produced in discovery. Individuals so authorized under an NDA may be individuals that the parties wish to include, and can agree to include, as authorized individuals under the protective order. While actual or alleged conduct of an individual during or after the trade secret sharing process may weigh in favor or against such authorization under the protective order, the main point here is that individuals authorized under the NDA may provide a basis for resolving the ancillary dispute.

[28] *See* note 7, *supra*.

[29] *See, e.g.,* Abrasic 90 Inc. v. Weldcote Metals, Inc*.,* 364 F. Supp. 3d 888, 898 (N.D. Ill. 2019) ("Failure to enter into nondisclosure or confidentiality agreements often dooms trade secret claims."). While not necessarily cast as such, an NDA is one of three common-sense, usually easily achievable protective measures that judges and juries readily understand and often expect to see. The other two common-sense, usually easily achievable protective measures are (1) marking as "trade secret," "secret" or "confidential" a document or file that is or includes a trade secret, thereby providing notice of the information's status to those who access it and (2) limiting trade secret acquisition, access, disclosure and use to those persons with a need to know the trade secret. Having said that, there is no mandatory protective measure(s) or tool(s) that must be implemented for information to have trade secret status.

[30] An integration clause is sometimes called a merger clause or entire agreement clause.

signed and any trade secret is shared because trade secret sharing, i.e., disclosure, can be the classic example of being unable to "un-ring" the bell, or requiring significant efforts to correct or limit actual and potential consequences. In short, an overall goal is to enter an NDA that is compatible with, and avoids a breach of or conflict with, relevant existing and anticipated agreements, relationships and litigation.

a. Definition of "Trade Secrets"

NDAs often define information being shared as "Confidential Information" and often include the term "trade secrets" within that definition. That approach may be convenient, but it often does not sufficiently focus the parties' attention on the categories of trade secrets to be shared. Thus, parties who are about to share trade secrets should consider defining the term "trade secrets" in an NDA, and that is true even if they decide to define and account for "confidential information" and include "trade secrets" within the definition of "confidential information."[31]

Parties may have opposing views on how to define "trade secrets" in an NDA. For example, the disclosing party may want a broad definition of the categories to be shared, given that it wants to protect by contract as much of the shared information as possible. Conversely, the receiving party may want a narrow definition so that, for example, it is not broadly obligated or impaired or foreclosed from present or future activity in a certain field. Other times, both parties may want to narrowly define "trade secrets" so that the sharing is focused and notice regarding the respective rights and obligations is correspondingly clear. In other words, a focused definition should facilitate the disclosing party's efforts to collect and organize the trade secrets to be shared and result in the disclosure, receipt and management of fewer trade secrets. Where fewer trade secrets are at issue, the parties may save time, money and effort during the sharing and the overall risk, degree of potential harm and potential for a dispute may be reduced.

Notably, an NDA, like most contracts, typically provides a mechanism for the parties to amend a term or provision, such as the definition of "trade secrets." Bear in mind, however, that no matter what the definition of "trade secrets" is, or is amended to be, no trade secret should be identified in that definition or elsewhere in the NDA. Such identification should be avoided because it can risk unprotected exposure and loss of the trade secret. More specifically, a person who needs to acquire, access, review, disclose or use an NDA in connection with an administrative function, such as contract management, often does not need to acquire, access, review, disclose or use, i.e., does not need to know, a trade secret. The definition of "trade secrets" also can include a procedural component. That is, a disclosing party typically is obligated to mark a shared trade secret in a particular way so

---

[31] The definition of "trade secrets" addressed here is a subject matter definition where the categories of the trade secrets are described. The legal definition of "trade secret" is not being restated or otherwise modified. As discussed herein, the legal definition is being applied. The applicable legal definition, whether under the DTSA, a State's version of the UTSA or otherwise, can be accounted for in a choice of law provision within the NDA or would be determined during trade secret litigation or an ADR process.

that the disclosing party knows what trade secrets are disclosed and the receiving party knows what trade secrets it receives just by looking at the document or file.

Additionally, an NDA can exclude information from the definition of "trade secrets." For example, "trade secrets" would not include information that is or becomes generally or publicly known through no fault of the receiving party.[32] However, if a trade secret becomes generally or publicly known, how that situation unfolded and who is at fault may not be clear. One way for the disclosing party to potentially improve its ability to obtain relief under such circumstances is a provision where (1) the receiving party's specific protective measure obligations are listed and (2) the receiving party is obligated to protect the shared trade secrets with measures of protection that meet or exceed the measures it uses to protect its own trade secrets or, if it has no trade secrets, then its most important confidential information. The specific protective-measure obligations can provide a useful roadmap to investigate, determine and prove fault. So, too, can the protective measures used by the receiving party, especially if those measures likewise are listed in the NDA itself or set forth in an addendum to the NDA.

An NDA also can exclude from the definition of "trade secrets" information that was or is independently developed by the receiving party, i.e., developed without the use of the disclosing party's trade secrets, or previously known by the receiving party, i.e., known prior to the date the trade secrets were shared. *See, e.g.*, 18 U.S.C. § 1839(6)(B). Such an exclusion also may be supplemented by a corresponding provision specifying how, and possibly a date by which, a receiving party can or must claim that it previously independently developed or knew certain information.

Likewise, an NDA can exclude from the definition of "trade secrets" information that was or is reverse engineered by the receiving party. *See, e.g.,* 18 U.S.C. § 1839(6)(B). However, a disclosing party may need to carefully consider whether such an exclusion is tenable. For example, where a shared trade secret is a prototype, product, service, component or other item that is not commercially available, such an exclusion may unnecessarily provide an opportunity or defense for the receiving party.

The above discussion about the definition of "trade secrets" illustrates the need to carefully draft and review an NDA and tailor it to the specific circumstances at issue. This is not to say that certain terms or provisions, such as a provision for amending an NDA, may not be relatively standard or common. But accepting boilerplate terms or provisions, which may be presented as take it or leave it, can be costly.

Moreover, a failure to include any exception to or exclusion from the definition of "trade secrets" may erode the enforceability of the definition and, by extension, the NDA in any litigation.[33] Taking into account the above discussion, an example of such an exception or exclusion is information that

---

[32] *See, e.g.,* 18 U.S.C. § 1839(3)(B).

[33] *Cf.* Orca Communications Unlimited, LLC v. Noder, 314 P.3d 89, 94-95 (Ariz. App. Ct. 2013) ("The difficulty here is that the Agreement's definition of 'confidential information' extends far beyond the 'truly confidential.' . . . The definition's overbreadth makes the confidentiality covenant unenforceable.").

verifiably (1) was publicly or generally known prior to the sharing, (2) was known to the receiving party prior to the sharing, or (3) became known to the receiving party after the sharing, but not through a person who owed a duty of confidentiality to the disclosing party.

b. The Parties to the NDA

Another issue that often arises when negotiating an NDA is who—which entities and which individuals—will be parties to or otherwise bound by its terms. Where, for example, a transaction involves only two parties, i.e., one disclosing party and one receiving party, where each party is organized and operating in uncomplicated fashion, e.g., both are single-location companies with no affiliates, resolution of this issue can be relatively straightforward. However, where, for example, a transaction involves multiple parties organized and operating in complicated fashion, resolution of this issue can require greater inquiry and attention to detail and more specific NDA provisions. The parties should address, early in negotiations, their respective organizations and operations, including locations and affiliates, and which persons—e.g., affiliates, employees and other entities and individuals—will be parties to the NDA or otherwise bound by its terms. A person otherwise may be bound by, for example, a written, executed addendum to the NDA, a copy of which can be provided in timely fashion to the disclosing party. Where multiple locations are in play because, for example, the disclosing party and receiving party are located in different jurisdictions, the parties can address basic but important issues, such as choice of law and forum and venue selection in the event a subsequent dispute arises.[34] Where multiple locations are in play because, for example, an authorized affiliate or employee of the receiving party is in location X and another authorized affiliate or employee of the receiving party is in location Y, then the disclosing party should consider whether either location or jurisdiction poses challenges that can be resolved or should be avoided. Those challenges may relate to enforcement of the NDA, or a certain provision therein, in the event a subsequent dispute arises.

c. The Purpose for Sharing Trade Secrets

A key provision in an NDA is a provision that specifies the purpose for sharing trade secrets. Parties to an NDA often include a provision specifying the purpose for sharing trade secrets, stating the period during which the sharing can take place and limiting any acquisition, access, review, disclosure and use of shared trade secrets to the specific purpose. As discussed above, a typical purpose is to evaluate a potential future relationship between the parties, such as a license, sale of assets, merger or acquisition. Any acquisition, access, review, disclosure or use of a shared trade secret outside that purpose or for another purpose, such as advancing the receiving party's own commercial interests, can be prohibited. Also, the parties can include an NDA provision specifying the receiving party's receipt of and authorized activity relating to the shared trade secrets is not intended to create and does not create a commitment to enter a subsequent relationship with the disclosing party. Indeed, a receiving party may require such a provision because it is or may be assessing, or may want to maintain its ability to assess, one or more other relationships with persons other than the disclosing party. A disclosing party can assess whether such a requirement and any underlying circumstances can be

---

[34] These issues are further discussed below.

adequately accounted for in the NDA and otherwise or whether the requirement and circumstances make sharing trade secrets with the receiving party too risky to proceed. An NDA provision that might address some of the disclosing party's concern and limit some of the risk is a provision specifying that the receiving party promptly notify the disclosing party, in writing, when it decides to end due diligence and not continue to a relationship with the disclosing party. Armed with that knowledge, the disclosing party can then take corresponding steps in timely fashion to protect its trade secrets and other interests.

d. Specifying Physical and Technological Tools

An NDA, i.e., a contractual tool, is typically not the exclusive means to protect shared trade secrets. Physical and technological tools, which are addressed in detail below, also are typically used. NDA provisions, or an addendum to the NDA, can specify the physical and technological tools to be used to protect shared trade secrets. Ultimately, those physical and technological tools complement, embody and implement NDA provisions relating to acquisition, access, review, disclosure, use and protection of shared trade secrets.

e. How Trade Secrets Can Be Acquired, Accessed, Reviewed, Disclosed and Used

An NDA also can set forth how the receiving party can acquire, access, review, disclose and use shared trade secrets. A provision addressing these issues can (1) set forth the points or locations and other details, such as channels and means, for authorized individuals to acquire, access, review, disclose or use trade secrets and (2) describe or identify specific individuals authorized to acquire, access, review, disclose or use trade secrets. An NDA also may specify that individuals so authorized must verifiably acknowledge—e.g., in writing or by click—applicable obligations each time any such act occurs.

An NDA also can include a provision with additional prohibitions or limitations on when, where, why, how and by whom shared trade secrets may be acquired, accessed, reviewed, disclosed and used.[35] Typically, only an individual with a need to know a trade secret should be authorized to engage in any such activity. To that end, individuals, by name, title or category, with need-to-know status and such authority can be specified in an NDA, as suggested above, as can individuals, by name, title or category, who lack such status and authority.

---

[35] As discussed above, an NDA can include a provision stating the purpose for sharing trade secrets. The "why" here entails a provision that, for example, prohibits or further limits a specific individual's or specific individuals' acquisition, access, review, use and disclosure of trade secrets based on the timing or reason(s) for doing so.

f. Temporal or Durational Limitation on Confidentiality Obligations

An NDA may include a temporal restriction or durational limitation on confidentiality obligations, it may provide that those obligations continue so long as at least one shared trade secret remains secret, it may provide that those obligations continue on a per trade-secret basis, i.e., with respect to a trade secret for so long as the trade secret remains secret, or it may provide that those obligations continue in perpetuity. Parties should be aware that some courts may view an NDA as a contract that can negatively impact competition and, as such, may look skeptically at a confidentiality obligation without a durational limitation.[36] Having said that, some trade secrets can exist forever, i.e., they can exist until they are no longer secret, other trade secrets may have a shelf life because once executed they become public—in the case of a marketing strategy, for example—and other trade secrets may, after a period of time, become stale and have no value—in the case of cost or pricing data, for example. A key point here is that any temporal restriction or durational limitation must be carefully assessed by both parties, and especially the disclosing party, as it can have a significant impact on trade secret status and the parties' respective rights and obligations. Evaluating the heft of obligations, if any, upon termination or expiration can be an important balancing exercise so as not to import too rigorous or too lenient conditions on protective trade secrets, particularly those that may undermine one's efforts to reasonably protect trade secrets.

g. Return or Destruction of Trade Secrets

An NDA can include a provision addressing how the termination of the parties' due diligence or relationship affects the NDA. The provision may state that confidentiality and other obligations continue, despite termination, and that the receiving party must take certain steps to protect shared trade secrets, including, for example, returning or destroying the trade secrets in its possession, custody or control. Importantly, an NDA can include a provision requiring the receiving party to acknowledge, in a signed writing, the specific trade secrets returned or destroyed and that no copy of, and no file or document containing, based on or derived from, any trade secret has been retained. As a practical matter, a return or destruction obligation is an obligation of which the disclosing party can affirmatively remind the receiving party once the due diligence or relationship is terminated. Also, an NDA may set forth exclusions to the return or destruction obligation, such as: (1) documents or information that must be retained by the receiving party in order to comply with an applicable legal or regulatory obligation, with such return or destruction promptly occurring upon termination of the legal or regulatory obligation, (2) document or information back-ups in the ordinary course that are not accessible by any unauthorized person, where such back-ups will be destroyed, or permanently deleted, in the normal course of the receiving party's document retention or

---

[36] *See, e.g.,* Carlson Grp., Inc. v. Davenport, No. 16-CV-10520, 2016 WL 7212522, at *5 (N.D. Ill. Dec. 13, 2016) (invalidating a nondisclosure clause as unreasonable and noting that the omission of a temporal limitation bears on its reasonableness.) *But see, e.g.,* 765 ILCS 1065/8 (b) ("This Act does not affect: (1) contractual remedies, whether or not based upon misappropriation of a trade secret, provided however, that a contractual or other duty to maintain secrecy or limit use of a trade secret shall not be deemed to be void or unenforceable solely for lack of durational or geographical limitation on the duty").

destruction policy, a copy of which the receiving party has provided to the disclosing party for further, calendared follow-up, for example, (3) where a dispute between the parties exists, documents or information relating to, or that reasonably may relate to, the dispute may be retained by the receiving party's outside counsel until the dispute is fully and finally resolved, after which return or destruction promptly occurs or further retention is subject to conditions set forth in, for example, a protective order or settlement agreement, and (4) limited C-suite-level or Board-level documents or information, such as meeting minutes, with any such documents and information subject to corresponding protective measures, including limited access and redaction obligations, and destroyed, or permanently deleted, in the normal course of the receiving party's document retention or destruction policy, a copy of which the receiving party has provided to the disclosing party for further, calendared follow-up, for example.

Further, proper return or destruction of trade secrets can be undermined where the event triggering the return or destruction and the date by which to do so is not clearly set forth in the NDA. Specifying an event, such as written notice or a due diligence or relationship milestone, is one way to specify a triggering event and the corresponding date for return or destruction.

h. Remedies

An NDA can specify remedies for a breach of the NDA. Relatedly, an NDA can include three provisions that impact the availability of those remedies: (1) a pre-litigation dispute process; (2) choice of law; and (3) selection of forum and venue.

Pursuant to a pre-litigation dispute provision, the parties may be required to attempt to resolve any dispute, such as a claimed breach, prior to commencing litigation or other dispute resolution process.[37] While each situation is unique, a disclosing party may be hesitant to agree to a time-consuming or involved pre-litigation dispute process, especially considering the relative fragility of trade secrets.[38] Indeed, even where an NDA includes a pre-litigation dispute provision, a disclosing party often will seek a provision that allows it, at any time, to seek a temporary restraining order and preliminary injunction for actual or threatened misappropriation. In contrast, a receiving party may be content with a pre-litigation dispute provision that requires relatively involved efforts to resolve any dispute prior to commencing litigation.

Pursuant to a choice of law provision, the parties can specify the State law that will govern the interpretation and enforcement of the contract and the law that will govern a trade secret claim or issue. An informed choice of law decision will account for the validity and enforceability of NDA

---

[37] For example, a disclosing party may claim that a receiving party breached an NDA by failing to comply with a protective measure requirement, such as a requirement to implement a specific contractual, technological or physical tool. The NDA may specify a notice, inspection and cure process for the claimed breach, consequences for the claimed breach if not cured and remedies for a breach proven in litigation.

[38] Kinship Partners, Inc. v. Embark Veterinary, Inc., 3:21-cv-01631-HZ, at *17 (D. Or. Jan. 3, 2022) ("A trade secret once lost is, of course, lost forever.")

provisions under the chosen law. As discussed above, some courts applying some States' laws may scrutinize and limit an NDA because of anti-competitive effects, just as those courts would scrutinize, for example, a noncompete or non-solicitation agreement or provision (noncompetes and non-solicits). The same can be said for an ADR forum, such as an arbitrator, a panel of arbitrators or a mediator. A trade secret claim may be brought under federal law, i.e., the Defend Trade Secrets Act (DTSA), or state law, i.e., a State's version of the Uniform Trade Secrets Act (UTSA) or New York common law. A trade-secret claim generally comprises the same or similar elements under the DTSA, UTSA and New York law, although interpretation and application of those elements can differ according to the jurisdiction. Certain claims, such as inevitable misappropriation, are available only under certain trade secret laws. Certain remedies may be available under only federal or a certain State's trade secret law. Extraterritorial application of the law at issue can also vary and factor in the choice of law decision.

With respect to a forum and venue-selection clause, the primary issue is whether a court, including a jury, or an ADR forum, will hear and decide a dispute. A forum and venue-selection clause often mandates a single forum and venue for any dispute between the parties that arises out of or relates to the NDA.[39] ADR may be an attractive process for the receiving party because a claimed breach of the NDA, i.e., alleged bad acts, may be addressed in a confidential environment, such as arbitration, instead of in a publicly accessible courtroom and on a publicly accessible docket.[40] An arbitrator also may be less likely than a court to award injunctive relief. ADR may be an attractive process for the disclosing party because a confidential environment, such as arbitration, can make it easier to maintain the secrecy of an asserted trade secret. At the same time, the disclosing party may want a judge and jury to hear and decide its misappropriation case, with such a desire potentially more pronounced where substantial damages, enhanced damages or attorneys' fees are or may be in play. Of course, depending on the goals, circumstances and experience of each respective party and the nature of the interaction or transaction at issue, a given party's preference for a certain forum, venue and process may, at the time the NDA is entered, run counter to those general propositions. Another factor to consider is a party's familiarity with a particular forum, venue and process, and the forum's or venue's overall experience and body of case law relating to trade secret misappropriation. Finally, where the parties are domiciled and, in particular, the locations from which they operate also may factor into reaching an agreement on a forum and venue selection clause. One party may not wish to litigate a misappropriation case on the so-called "home court" of the other party, where the jury's and perhaps even the judges' familiarity with a party may create a home-court advantage. At the same time, the other party may wish to litigate a misappropriation case where, for example, certain witnesses and a physical facility are located.

---

39 *See* Paragon Micro, Inc. v. Bundy*,* 22 F. Supp. 3d 880, 891 (N.D. Ill. 2014) (compelling trade secret misappropriation case to arbitration), *citing* Shearson/American Exp., Inc. v. McMahon, 482 U.S. 220, 226, 107 S. Ct. 2332, 96 L.Ed.2d 185 (1987) ("This duty to enforce arbitration agreements is not diminished when a party bound by an agreement raises a claim founded on statutory rights.").

40 The arbitrability of a dispute—that is, whether a dispute is encompassed by an ADR clause—can be the subject of costly litigation before an arbitrator, court or both. So, if ADR is the parties' desired dispute resolution process, then clear, express terms about which disputes are to be so resolved should be used.

i. Other Documents, Including Other Agreements

In addition to an NDA, there are other documents that may be negotiated and exchanged between parties prior to sharing trade secrets. These documents may include (a) policies and procedures for employees of, or other individuals affiliated with, the receiving party who are authorized to acquire, access, review, disclose or use shared trade secrets and (b) as discussed above, acknowledgments, signed by those employees or other individuals, in which they acknowledge and agree to be bound by the NDA and accompanying policies and procedures.

The parties also may enter into agreements that protect against unfair competition, such as noncompetes or non-solicits. Noncompetes may proscribe the receiving party from engaging in certain competitive activity or lines of business while it possesses or can acquire, access, review, disclose or use the disclosing party's trade secrets, and for a period thereafter, which period may be based on or a proxy for an independent development period. Notably, if there is a dispute, the receiving party may argue that such a period is the maximum duration of any injunctive relief the disclosing party can seek and obtain.[41] Non-solicits may proscribe the receiving party, or both parties from, for example, soliciting and hiring key employees of the other party for a certain period.[42] Key employees authorized to acquire, access, review, disclose or use shared trade secrets also may enter noncompetes or non-solicits.

Notably, noncompetes and, relatedly, NDAs and non-solicits have been and are subject to increasing attention from, for example, Congress, the FTC, the National Labor Relations Board and certain State legislatures. That attention has resulted in state laws and proposed federal laws and regulations restricting, or, in some situations, banning noncompetes. Further, other agreements, such as NDAs and non-solicits, may be within the scope of some of those restrictions and bans, meaning that those other agreements may be challenged and invalidated or rendered unenforceable as overly broad. As such, parties should account for applicable, enacted laws and regulations and case law when it comes to noncompetes and other, related agreements. Additionally, non-solicits may raise antitrust or other competition considerations. Parties likewise should account for those considerations.

---

41 "[T]he most commonly employed standard [for calculating the duration of an injunction in a trade secret case is]: 'the period of time that would be required for independent development'" of the trade secret. ShowCoat Sols., LLC v. Butler, no. 01:18-cv-789-ALB, *11 (M.D. Ala. Mar. 19, 2020) (internal citation omitted). While the independent development period is sometimes referred to as the head-start period, the term head-start period is often used to identify the period within which a "[d]efendant's misappropriation gave it a leg up on the competition" and, as such, the period within which a plaintiff is entitled to damages. AMS Sensors U.S. Inc. v. Renesas Elecs. Am. Inc., no. 4:08-cv-00451, *11 (E.D. Tex. Feb. 26, 2021) (internal citations omitted).

42 A nonsolicit may be an agreement directed to certain customers, employees or a combination of those persons and prohibits a party to the agreement from, for example, soliciting those customers, employees or a combination of those persons. A non-hire, or non-poach, agreement may be an agreement directed to certain employees and prohibits a party to the agreement from, for example, soliciting and hiring certain employees.

2. Physical Tools

Physical tools are tangible, often readily visible measures, such as notices and barriers, for protecting trade secrets. A disclosing party, such as a trade secret owner, often uses physical tools to protect its trade secrets. At the pre-due diligence or pre-relationship stage, the disclosing party will not likely share identified trade secrets. So, at this pre-sharing stage, physical tools that the receiving party will be required to use during due diligence or a relationship—when the receiving party acquires, accesses, reviews, discloses and uses shared trade secrets—can be investigated and assessed and then specified in the NDA. Such physical tools can include the disclosing party's physical tools the receiving party will likewise need to maintain or implement. Such communication and, ultimately, cooperation can reduce the risk of physical tool deficiencies, mistakes, or failures, which can negatively impact an asset's trade-secret status. In some situations, the disclosing party may want the rights to inspect, approve and require supplementation or modification of the receiving party's physical tools to further reduce that risk and avoid any misunderstanding, ambiguity or conflict.

There are multiple physical tools available. Physical tools can be promulgated through contractual or other administrative tools, such as trade-secret policies and procedures. Training new or returning employees on those policies and procedures, including periodic refresher training and updated training, is an example of another administrative tool.

The use of any physical tool depends on the circumstances at issue and there often is a relation or overlap between contractual, physical and technological tools.[43] For example, an NDA may require that the paper version of the document be marked as "Trade Secret" or "Confidential" and the same information in electronic form, i.e., electronically stored information (ESI), be digitally marked in the same manner. Likewise, where an NDA may require that a document be stored in a locked room or

---

[43] Protective measures, i.e., all contractual, physical and technological tools, typically are considered together in assessing whether the measures have been and are reasonable. *See* Hertz v. Luzenac Group, 576 F.3d 1103, 1113 (10th Cir. 2009) (noting that "Luzenac took a series of steps to protect the secrecy" of its process and "there always are more security precautions that can be taken. Just because there is something else that Luzenac *could* have done does not mean that their efforts were unreasonable under the circumstances[;]" and holding that "whether precautions were, in fact, reasonable, will have to be decided by a jury") (emphasis in original); Surgidev Corp. v. Eye Tech., Inc., 828 F.2d 452, 455 (8th Cir. 1987) (explaining that "[o]nly reasonable efforts, *not all conceivable efforts*, are required to protect the confidentiality of putative trade secrets") (emphasis added); TouchPoint Solutions, Inc. v. Eastman Kodak Co., 345 F. Supp. 2d 23, 30-31 (D. Mass. 2004) ("But the standard is reasonableness, not perfection. . . . the [Confidential Disclosure Agreement's (CDA)] existence is some evidence of reasonable security measures. . . TouchPoint also put into place numerous other security measures. . . Kodak's response, that compliance or non-compliance with the CDA is dispositive of the reasonableness of security measures, would render the taking of all other precautions pointless. That is not the intent of the preferred inquiry."). Having said that, particular tools, i.e., one or more contractual, physical or technological tools, can be evaluated for reasonableness. Where trade secrets are to be shared, an evaluation of overall or particular tools can include the disclosing party's tools and the receiving party's tools. *See*, *e.g., TouchPoint,* 345 F. Supp. 2d at 30 ("even with a written CDA in place, the Court may examine the conduct of the parties to determine the scope of their confidential relationship and the reasonableness of their efforts to protect secrecy.")

safe, the paper version of the document may be stored in a locked room or safe, and the same ESI may be password-protected, encrypted and stored on a local hard drive in a locked room. Examples of physical tools used to protect trade secrets include:

- **Labeling, Printing and Copying**
    - Mark trade secrets with express, conspicuous labels, watermarks or legends, such as "Trade Secret" or "Confidential"
    - Use tracking devices or indicia
    - If printing or copying is allowed, print, or copy trade secrets on copy-proof or non-photocopiable paper
    - Use color-coded paper to identify a document containing a trade secret or a specific-colored paper for a specific document containing information at a certain level of confidentiality

- **Facility and Transport Security**
    - Secure trade secrets in one or more of locked drawers, filing cabinets, safes, or rooms
    - Mark areas containing trade secrets as "confidential," or with a similar designation
    - Control and restrict access to those marked areas
    - Store trade secrets in a secure area, such as an office or other room with a door, rather than a cubicle or open space
        - Maintain trade secrets in windowless rooms
        - Provide secure work areas where trade secrets can be acquired, accessed, reviewed, disclosed and used without exposure to others who are not authorized to engage in any such activity
        - Maintain access logs for anyone entering a secure area where trade secrets are stored, acquired, accessed, reviewed, disclosed, used, embodied, or in operation
    - Require key card or code access for employees and other authorized individuals, including levels of permission, especially for secure areas
    - Install gated, perimeter fences to keep out uninvited, unscheduled, or uncontrolled visitors
    - Install video surveillance cameras to monitor ingress to and egress from the facility, building, or secure area, such as where trade secrets are stored, acquired, accessed, reviewed, disclosed, used, embodied or in operation

- Install alarm systems
- Install bars on windows
- Employ security guards to verify visitors through, for example, a photo identification and to log and admit visitors at facility, building, or secure-area entrances
- Employ security guards and dogs to patrol the grounds during and after business hours
- Transport trade secrets via secure carriers and in locked, secure containers

- **Visitor Protocols**
  - Maintain logs of visitor entry and exit
  - Require visitors to be identified and badged when on premises
  - Require visitors to sign agreements not to acquire, access, review, disclose, use or remove any company information without permission
  - Escort visitors while in the facility, building or secure area
  - Search visitor bags when entering and exiting the facility, building, or secure area
  - Prohibit recording of any audio and video and taking of any photographs during visits by, e.g., collecting devices with any recording capability, such as a camera, and affixing security tape to cover any camera lens

- **Employee Obligations**
  - Employee manuals, policies and guidelines for trade secrets, in printed or ESI form, distributed to employees who sign and date acknowledgments of receiving, reading, and understanding those materials. Such materials can include corresponding explanations of:
    - What trade secrets are, such as by categories of information, and how they are marked and protected and
    - Who can, i.e., is authorized to, acquire, access, review, disclose, or use trade secrets, with whom they can discuss and to whom they can disclose trade secrets, and to what extent and under what circumstances or conditions such discussions and disclosures can occur
  - Treatment of a third party's trade secrets, including segregation from the company's trade secrets
  - Instructions on storage of trade secrets, including securely storing lab notebooks in, for example, a locked area or desk and password protecting e-lab notebooks, and not

leaving the lab notebook unattended in an area or on a desk or opened on an unattended laptop, tablet or other device

- Travel protocols, such as using privacy screens on approved or issued travel devices, including laptops and tablets, not leaving any devices unattended or unsecured, and not taking trade secrets with you, whether on a laptop, tablet, or other device
- Protocols for the return or destruction by, for example, shredding or deleting, of any embodiment or copy of a trade secret where the embodiment or copy is no longer needed, the need to know the trade secret ceases or the authority to access the trade secret is terminated, including upon employment termination or furlough, whether voluntary or involuntary
- Protocols for securing a trade secret when off-site, including when at home, working remotely or traveling, if off-site trade secret access or related activity is authorized by, for example, securing it in a locked office or filing cabinet or on a password-protected, authorized laptop, tablet, or other device and in a password-protected file
- Incident response plan to address actual, potential, or suspected trade secret misappropriation, including any unauthorized acquisition, access, review, disclosure or use or related activity, events or issues
- Obligations under and responsibilities and roles in an incident response plan, including procedures for timely reporting any actual, potential, or suspected (i) breach of a policy or procedure for protecting trade secrets or (ii) unauthorized acquisition, access, review, disclosure, or use of a trade secret
- Initial, refresher, and updated training sessions for new, returning, and existing employees[44]

3. Technological Tools

A disclosing party often uses technological tools to protect its trade secrets. As with physical tools, technological tools can be promulgated through administrative tools, such as policies and

---

[44] *See, e.g.,* MicroStrategy Inc. v. Business Objects, S.A., 331 F. Supp. 2d 396, 403, 420 (E.D. Va. 2004) (finding MicroStrategy "took reasonable steps to preserve the secrecy of its information" by having, among other things, "physical security, such as locked doors, limited access to its buildings through the use of badges, and the use of security cameras"); U.S. v. Shanshan Du, 570 Fed. Appx. 490, 500 (6th Cir. 2014) (reasonable measures included physical security such as "a locked facility monitored at all times by security guards, who required employees to show a photo identification to enter . . . guards checked all bags and computer devices carried out of the building, patrolled the facility after hours, and escorted visitors within the facility"); U.S. v. Hanjuan Jin, 883 F. Supp. 2d 977, 998-99, 1008 (N.D. Ill. 2012) (reasonable measures included security officers, cameras, alarms and gated car access with key card); Smithfield Packaged Meats Sales Corp. v. Dietz & Watson, Inc., 452 F. Supp. 3d 843, 858 (reasonable measures included physical security such as "codes, badges, or fobs to access its physical offices and plants, and requir[ing] visitors to sign agreements preventing them from removing information from offices and plants"). *See also* 1 Corp Couns Gd to Tech Mgmt & Trans §§ 6:1, 6:14-6:24; *and* https://www.uspto.gov/sites/default/files/documents/CRS-LA-OBrien-trade-secrets.pdf.

procedures, including employee training. At the pre-due diligence or pre-relationship stage, the disclosing party will not likely share its trade secrets. So, at this stage, technological tools that a receiving party will use during due diligence or a relationship—when the receiving party acquires, accesses, reviews, discloses or uses shared trade secrets—can be investigated and assessed and then specified in an NDA. Such technological tools can include the disclosing party's technological tools that the receiving party will likewise need to maintain or implement. Such communication and, ultimately, cooperation can reduce the risk of technological tool deficiencies, mistakes or failures, which can negatively impact an asset's secret status. In some situations, the disclosing party may want the right to inspect, approve and require supplementation or modification of the receiving party's technological tools to further reduce that risk and avoid any misunderstanding, ambiguity or conflict.

Importantly, contemplated or actual use of technological tools can create the impression that the disclosing party agrees to electronically share all the trade secrets to be shared. In fact, a disclosing party may agree to share one or more trade secrets, initially or thereafter, only in physical or paper form and only in a secure physical location where contractual and physical tools are utilized. Under such circumstances, the use of technological tools may not be necessary.

The disclosing party should be well prepared, based on its own operations and technological tools, to specify the technological tools the receiving party needs to maintain, implement, supplement, or modify. Indeed, in the modern, remote world, trade secrets often are electronically created, stored, acquired, accessed, reviewed, disclosed and used by the disclosing party.[45] That electronic activity occurs on and through a variety of systems, equipment, devices and media, such as proprietary databases, shared folders and drives, cloud systems, email and other communication platforms, portals, such as VPNs, on-site computers and remote computers, including laptops, tablets and smartphones. The disclosing party's awareness of its trade secret-related electronic activity, systems, equipment, devices and media, as well as the corresponding technological tools it utilizes, should significantly inform its technological tool requirements for the receiving party.

For example, the disclosing party may have to decide whether to provide the receiving party access to its platform or portions thereof. If such access is provided, then the disclosing party can determine the credentials needed to gain access and the manner in which, including the device or devices through which, access will be permitted. Where appropriate and possible, the disclosing party also can test or conduct a dry run of, or periodically audit or evaluate, the access protocol to ensure it functions properly and to identify and troubleshoot vulnerabilities or risks, including those that may have been unanticipated or overlooked.

Overall, the disclosing party can keep in mind four important platform-related issues: (1) whether the platform is sufficiently secure, such that trade secrets can be shared with tolerable or minimal risk of misappropriation by unauthorized persons, whether affiliated with the receiving party or not, (2) whether the platform is configured to allow access to trade secrets on only a need-to-know basis,

---

[45] Trade secrets that are electronically created, stored, acquired, accessed, reviewed, disclosed and used by the disclosing party also are subject to technological threats.

i.e., to only authorized individuals,[46] (3) whether the platform is configured to allow access on only certain days and at only certain times, and (4) whether the platform is configured to monitor who accessed what trade secrets, when and by what means and to monitor other activity, such as downloading and printing, assuming such other activities, or functions, are enabled and permitted.[47] Addressing those issues before sharing trade secrets can help ensure that those measures properly are in place and operational when the trade secret sharing takes place.

Importantly, the disclosing party can consider and address essentially the same above four issues if it will be establishing a data or due diligence room—including one that is or includes a clean room—for trade secret sharing. Such rooms are further discussed below.

There are multiple technological tools that the disclosing party can use to protect trade secrets or, if segmented, portions of trade secrets, that are in electronic or digital form. Some of those tools can be used, or inform the tools to use, when protecting shared trade secrets. Examples of those tools include:

- **Password Protection and Encryption**
    - Password-protect documents, files, folders, and devices that are or contain trade secrets
    - Require complex passwords with frequent change intervals and password storage protocols, including storage in physically secured drawers or encrypted virtual password lockers
    - Use two- or multi-factor authentication technologies for trade-secret access
    - Encrypt at rest and in transit: encrypt documents, files, and folders that are or contain trade secrets when they are stored and if they are transmitted, and encrypt devices, hard drives and memory devices on or in which a trade secret is stored

- **Activity Tracking**
    - Maintain computer logs that track trade secret access by, for example, a trade secret identifier, such as a sequential number that does not disclose the trade secret, the name of the accessing person, and the date and time of platform, network, folder, file log in/log out, and access to/access out

---

[46] Failing to limit trade secret access to only those individuals who need to know the trade secrets in connection with the due diligence or relationship can be evidence that the trade secrets were not reasonably protected. *Cf.* George S. May Int'l Co. v. Int'l Profit Assocs., 256 Ill. App. 3d 779, 783, 628 N.E.2d 647, 650 (1st Dist. 1993) (holding that information was not a trade secret where it was disclosed without a confidentiality agreement to employees of plaintiff, which experienced a turnover of 600 employees annually); *see also* UTSA, §1, comment.

[47] Such monitoring may produce key evidence in a subsequent trade secret misappropriation, breach of contract or other dispute.

- Maintain computer logs tracking the device used to access a trade secret
- Maintain computer logs of any trade secret downloading, uploading, copying, printing, attaching, e-mailing, including forwarding, saving/saving as, revising or deleting, bearing in mind that all such functionality often can be permanently disabled
- Generate alerts on detection of any, or an abnormal volume or timing of, trade secret downloading, uploading, copying, printing, attaching, e-mailing, including forwarding, saving/saving as, revising or deleting, optionally with threshold generating interruptions of acquisition, access, review, disclosure and use of a trade secret

- **Limiting Access**
  - Limit remote access to the computer network, platform, folders or files that are or contain a trade secret
  - Allow access to a trade secret only from authorized devices, such as company-issued desktops, laptops and tablets
  - "Fingerprint" files that are or contain a trade secret with a marker, such as a typographical error or other benign error or content, to more easily prove trade secret misappropriation or breach of contract if that ever becomes necessary
  - Disable data ports on computers to prevent downloading or uploading trade secrets onto a remote memory device or other memory or storage medium
  - Adopt cyber-security protocols
    - Quarantine excessive or suspicious e-mail traffic
    - Limit or prevent access to social media accounts
    - Limit or prevent access to certain websites
    - Install and update malware and anti-virus software
    - Include, in an incident response plan, a response to any intrusion attempt or cyberattack, including individuals' responsibilities and roles and steps to be taken
  - Secure and verifiably erase trade secrets in electronic, digital, or magnetic memory after need for that copy has ended or memory is replaced or redeployed
  - Maintain trade secrets on computers or servers electronically, but physically disconnect the computers or servers from internal or external networks, including any WIFI or internet connection or access
  - Limit source-code sharing to secure, third-party escrow services that have proper access controls and limit or prohibit any downloading, uploading, copying, and printing of that code

- Ensure vendors and other business partners implement and comply with protective measures[48]

[48] *See* 1 Corp Couns Gd to Tech Mgmt & Trans §§ 6:1, 6:14-6:24; https://www.uspto.gov/sites/default/files/ documents/CRS-LA-OBrien-trade-secrets.pdf. *See also* Arkeyo, LW v. Cummins Allison Corp., 342 F. Supp. 3d 622, 630-32 (E.D. Pa. 2017) (no trade secrets in source code that plaintiff published on the internet for fifteen months without employing standard industry protections, e.g., there was no encryption, password protection, code obfuscation or confidentiality provisions or requirements that users abide by any terms; court observed that "Arkeyo committed the cyber equivalent of leaving its software on a park bench.").

V. CONSIDERATIONS WHEN SHARING DURING DUE DILIGENCE OR A RELATIONSHIP

A. Identify Assets At Issue

Principle No. 5: Sharing trade secrets is an attentive process where a disclosing party identifies a trade secret when it is shared and the disclosing party and receiving party protect the shared trade secret.[49]

Principle No. 6: Sharing trade secrets is an attentive process where a disclosing party, on its own or in collaboration with a receiving party, can provide and update categories of to-be-shared or shared trade secrets, identify additional shared trade secrets, specify shared trade secrets returned or destroyed by the receiving party and specify and update entities and individuals who are or are not authorized to acquire, access, review, disclose or use the shared trade secrets.

Issue No. 1: If a trade secret is not properly identified when it is shared, then potential consequences are:

(a) The trade secret—i.e., subject of the disclosing party**'**s and receiving party**'**s protective efforts—may not legally exist and trade secret status may be lost;

(b) The receiving party lacks notice of the trade secret requiring protection, thereby resulting in compromised secrecy and potential loss of trade secret status*;*

(c) An inaccurate valuation of the trade secret and, as a result, a lower economic return on the trade secret;

(d) Less control over, and reduced ability to track, the receiving party**'**s acquisition, access, review, disclosure and use of or to the trade secret, and post-due diligence or post-relationship, return or destruction of the trade secret;

(e) Inadvertent sharing of other information, including other trade secrets. In other words, a disclosing party should not disclose more than necessary and a receiving party likewise should not want to receive more than necessary. Corresponding, respective concerns include loss of trade-secrecy status for inadvertently disclosed trade secrets and potential exposure to claims that were not contemplated;

---

[49] The Sedona Conference, *Commentary on the Proper Identification of Asserted Trade Secrets in Misappropriation Cases*, 22 SEDONA CONF. J. 223 (2021), substantively analyzes the standard for proper trade secret identification, i.e., sufficient particularity, and provides examples of proper trade secret identification.

(f) Difficulty in identifying, or failing to identify, joint developments or modifications and corresponding rights and interests;

(g) Difficulty in pursuing a trade-secret misappropriation claim against the receiving party or a third party; and

(h) Increased difficulty in proving, by clear and convincing evidence, a prior commercial use defense under 35 U.S.C. § 273 and, in particular, the subject matter to which the defense applies.

The identification process can include the receiving party identifying its related or similar trade secrets, communicating and verifying that it possessed a disclosed trade secret prior to disclosure and separating pre-existing or ongoing work from the parties' relationship.

The receiving party also can confirm the disclosing party's measures to protect the shared trade secrets and prevent transfer of any trade secret rights, whether outright or through derivative works, to another person.

1. Identification Of Trade Secrets Shared

The transition to due diligence or a relationship typically warrants a correspondingly heightened protocol for sharing trade secrets, i.e., a stricter protocol than may have been used for pre-due diligence or pre-relationship sharing of a list of categories of the trade secrets. In other words, trade secrets likely were not and, absent reasonable measures to protect the trade secrets, should not have been shared before due diligence or a relationship. During due diligence or a relationship, trade secrets will be shared, and corresponding identification obligations of the disclosing party and confidentiality obligations of the receiving party will need to be fulfilled for the due diligence or relationship to proceed.

Once due diligence or a relationship commences, existing obligations set forth in a prior agreement, such as an NDA, may not cease. Rather, all or some obligations may continue, to the extent sufficient and applicable, or they may be supplemented, modified or enhanced while accounting for the parties' focus on the commercial objectives of the due diligence or relationship and recognizing that a transaction, for example, may or may not come to fruition, change, evolve or terminate. Obligations may continue, for example, where a triggering event or condition in a prior agreement occurs or is satisfied. Obligations may be supplemented, modified or enhanced in a new agreement or in an addendum to a prior agreement.

As noted in Section IV, there are three major categories of protective measures for trade secrets before, during and after due diligence or a relationship: (1) contractual tools, (2) physical tools and (3) technological tools, as well as corresponding administrative tools, such as employee education and training. Trade secret owners should consider utilizing all three types of tools when protecting trade secrets during due diligence or a relationship. While tools can be organized into those three categories for ease of discussion, the different tools are, in practice, connected.

At the inception of due diligence, a disclosing party should possess a list of identified trade secrets it intends to share and know the tools that have been or will be implemented by the receiving party to protect the trade secrets. To be clear, a due diligence or relationship list of trade secrets can include the identified trade secrets, and that contrasts with a pre-due diligence or pre-relationship list of categories of trade secrets, which should not include the identified trade secrets. Alternatively, the identified trade secrets may be an addendum to the due diligence or relationship trade-secret list, with such an approach potentially facilitating more controlled disclosure of the shared trade secrets by the disclosing party and more controlled acquisition, access, review, disclosure and use of or to the shared trade secrets by the receiving party.

Additionally, a disclosing party should be mindful of contexts in which disclosure of trade secrets is occurring to consider whether they are consistent with the agreed-upon categories. If the parties have not previously agreed in writing on a category into which a to-be-disclosed or disclosed trade secret falls, then previously agreed to categories can be supplemented prior to disclosing the trade secret or upon realizing that the disclosed trade secret lacks a corresponding category. Such supplementation of categories can help to ensure accurate accounting of shared trade secrets.

Principle No. 7: Sharing trade secrets is an attentive process that can be part of a disclosing party's or receiving party's broader information governance and management process, where tools a receiving party is to use to protect trade secrets can be specified in a contract, such as an NDA.

As noted above, a common starting point, or first tool, for protecting trade secrets during due diligence or a relationship is a contract, such as an NDA, that limits acquisition, access, review, disclosure and use of or to trade secrets. During due diligence or a relationship, the parties may enter an NDA that continues, modifies or builds upon an existing NDA or another agreement. Notably, an NDA used in connection with due diligence typically will limit such trade secret activities to only evaluation of a possible future relationship. Further, an NDA used in connection with due diligence or a relationship may account for supplemental, modified or enhanced physical and technological tools to protect trade secrets shared during due diligence or a relationship.

The NDA often addresses both written and oral sharing, i.e., disclosure, of trade secrets. Oral sharing may occur during, for example, an interview, meeting or demonstration relating to due diligence or a relationship. Such sharing typically can be memorialized through a procedure in the NDA that allows post-sharing written identification of trade secrets. Other oral sharing may occur outside a scheduled interview or meeting. For example, a receiving party may seek, and a disclosing party may provide extemporaneous supplemental or clarifying information because of human error, i.e., a trade secret may have been insufficiently identified when initially shared. Regardless of the circumstances, any oral sharing may be subject to differing interpretations or recollections. So, as a general proposition, oral sharing often is not preferred. But if it does occur, it can be promptly and accurately memorialized in writing pursuant to the agreed upon procedure.

Pursuant to the NDA, progressive, incremental sharing can be an appropriate approach. Under this approach, trade secret sharing will be gradual and contained. For example, (1) only trade secrets in a certain category or categories initially will be shared, (2) only a representative trade secret or representative trade secrets in each category initially will be shared, (3) only a very limited number of persons initially will be authorized to acquire, access, review, disclose and use the trade secrets and (4) time constraints will be placed on stages of acquisition, access, review, disclosure, use and, ultimately, evaluation of the disclosed trade secrets. Then, if there is mutual interest in continuing the process towards, for example, a relationship—the sharing— including the number of authorized persons and duration of authorization, can incrementally progress. Notably, progressive, incremental sharing can allow parties to more easily terminate the due diligence and part ways.

Confidentiality obligations in an NDA often are mutual. That two-way street accounts for a common dynamic of information sharing. Specifically, during due diligence or a relationship, a disclosing party often becomes a receiving party and vice versa. For example, the receiving party, prior to receipt of a trade secret from the disclosing party, may have conducted its own research or development relating to information it receives. To establish its rights and interests, the receiving party will share its information with the disclosing party. The receiving party also may have third-party obligations that require it to obtain mutual confidentiality obligations. Thus, while due diligence or a relationship initially may focus on rights and obligations that protect a disclosing party's trade secrets, there often is a need for corresponding rights and obligations to protect the receiving party's trade secrets, and sometimes a third party's trade secrets, that also are shared during the due diligence or relationship.[50]

Mutual sharing of trade secrets or related information also may occur—and corresponding protections are therefore appropriate—where new trade secrets may be jointly developed or existing trade secrets may be modified. Notably, confidentiality obligations relating to shared, jointly developed or modified trade secrets can continue where due diligence ends without a subsequent relationship, such as a licensor-licensee relationship, or where the subsequent relationship terminates.

Unsurprisingly, a receiving party often seeks to limit the duration of confidentiality obligations and, in effect, put a shelf-life on the trade secrets at issue. Such limitations typically conflict with the desire of a disclosing party. The disclosing party often wants confidentiality obligations to continue in perpetuity or until the trade secret becomes generally or publicly known through no fault of the receiving party. Sometimes there is room for compromise as to certain trade secrets. For example, a trade secret may have a natural shelf-life because it will be publicly or generally known when executed (e.g., a marketing plan) or comprises data (e.g., cost or pricing data) that is time-sensitive, meaning data that loses its value or becomes stale as time passes and market conditions change.

---

50 *See* Edifecs Inc. v. TIBCO Software, 756 F. Supp.2d 1313 (W.D. Wash. 2010). *Cf. Big Vision Private Ltd v. E.I. DuPont de Nemours & Co.*, 1 F. Supp.3d 224 (S.D.N.Y. 2014), *aff'd* 610 Fed. Appx. 69 (2nd Cir. 2015) (trade secret owner unable to enforce alleged trade secrets because it failed to give potential joint venturer, who also had been developing technology in the same area, clear notice of trade secrets shared).

Additionally, the parties may agree to treat trade secrets differently than other confidential information when it comes to the duration of confidentiality obligations.

During due diligence, information frequently is shared through a data room. Depending on the limitations on access to the room and the information stored in the room, a data room can be or include a clean room. Whether one is considering a physical, i.e., in-person, virtual, i.e., remote, or combined physical and remote data room, trade secrets in the data room can be protected (1) with the tools addressed in Section IV.C. above and (2) by requiring that persons authorized to access the data room and acquire, access, review, disclose or use the trade secrets not be involved in certain activities, such as research, development, engineering or patent prosecution, or with certain products or services, such as existing or planned competitive products or services.[51]

2. Identification Of Trade Secrets Or Other Assets Modified Or Jointly Developed

Principle No. 8: Sharing trade secrets can lead to the generation of additional, protectible assets, such as modifications to or derivations from those trade secrets and jointly developed trade secrets, the identification of and rights to which the parties can address in writing.

Where trade secrets are shared, related research, development and engineering efforts may take place. Sometimes those efforts are joint efforts and sometimes those efforts are parallel, independent, supplementary or complementary. A result of those efforts can be modifications, including improvements, to shared trade secrets, derivations from shared trade secrets and jointly developed, new assets, including trade secrets, all of which are topics that can be addressed in an agreement that governs the parties' relationship.

Also, just as pre-due diligence or pre-relationship protective measures, or tools, can be supplemented or enhanced as the parties transition into due diligence, such supplementation or enhancement can occur as the parties transition into a post-due diligence relationship. In other words, mutual and respective measures in effect during due diligence or pre-relationship often can continue, with appropriate modifications, into the relationship. The need for such continuation, with modifications, can be attributable to the parties' evolving interactions. Due diligence generally includes a sharing model comprising disclosure of trade secrets by the disclosing party, acquisition, access, review, disclosure and use of or to the trade secrets by the receiving party and discussions between the parties. In contrast, development work during a relationship typically is a more interactive process, with suggestions and collaboration that build on the parties' preceding activity.

---

[51] For additional guidance about Clean Rooms, *see* The Sedona Conference, *Commentary on the Use of Clean Rooms*, *Public Comment Version* (March 2025), *available at* https://thesedonaconference.org/publication/Commentary_on_Use_of_Clean_Rooms.

A key issue to address when it comes to modifications to or derivations from a trade secret is who owns the modified or derived subject matter, whether jointly developed or not. Parties can agree to joint ownership, where each party owns an undivided interest in the subsequently developed asset, with the right to sub-license. Another option is sole ownership by one party, with a license to the other party. The parties also may agree, as part of such an arrangement, that, if or while owner/licensor status is unresolved, each party shall have certain rights, such as a right to use the subsequently developed subject matter under certain conditions and for a certain term. The receiving party also may seek a feedback or residuals clause in the NDA or a related agreement. Under a feedback clause, the receiving party obtains, for example, a right to use, or even own, the feedback it provides to the disclosing party if the feedback modifies or improves the shared trade secret or other information, products, services or processes. Under a residuals clause, the receiving party has, for example, a right to use information, namely, general knowledge, that it received if such information is retained through unaided memory. The important point here is to timely contemplate and, if appropriate, timely address the issue of what rights, if any, attach to the fruits of the labor attendant to the sharing of trade secrets. A failure to do so can result in an avoidable and costly situation, including litigation or another dispute resolution process.

An important step in assessing whether subject matter is a subsequently developed asset is a complete and accurate list and identification of the trade secrets that each party has shared with the other party. Likewise, listing and identifying what is not being shared or included in a relationship can be important, especially if the parties' relationship, and corresponding agreements, have evolved from, for example, pre-due diligence to due diligence to post-due diligence relationship.

Additionally, there can be disclosure obligations where the party first aware of the subsequently developed asset discloses it to the other party. Such an obligation can be buttressed with corresponding audit and inspection rights, or even a portion of an incident response plan addressing steps to be taken where there is non-compliance or reason to believe there is non-compliance with applicable obligations.

In addition to defining ownership, control and maintenance of subsequently developed trade secrets and other assets, parties can specify in a joint development (or other agreement) other aspects of their relationship, such as the corresponding royalties or other compensation that will be due, the availability of and procedures for exercising audit and inspection rights, the effects of a change in ownership or control of either or both parties, and the reasons for and consequences of termination of the agreement or overall relationship. Parties also can specify which party, or parties, may apply for, own and enforce specific assets, such as patents, and cooperation or other obligations in connection with the application process and enforcement actions.[52]

Finer points for which the parties can account include timely documentation of trade secrets or other information each party has or has not contributed to a modified, derived or jointly developed trade secret or other asset and when any such contribution occurred. Timely documentation of a

---

52 *See*, *e.g.,* Lucent Techs., Inc. v. Gateway, Inc., 543 F.3d 710 (Fed. Cir. 2008)

contribution can facilitate progress of ongoing development work, often is important to establish legal rights and interests in and to the results of development work and can avoid, or reduce the time and expense of, a dispute that may develop between the parties. To those ends, parties can update the list and identification of trade secrets shared, as well as prepare and update a list of modified, derived or jointly developed trade secrets or other assets, as the relationship proceeds. Procedures for such updates, or preparation and updates, including timing and related audits and inspections, can be accounted for in a joint development or other agreement, and corresponding governance, compliance or oversight liaisons or committees may be part of such procedures. Compliance with such procedures can be a precondition to bringing or defending an action against the other party.

B. Updating Protective Measures When Sharing Trade Secrets

As the relationship between the parties evolves, it may become necessary to update the contractual tools to protect shared trade secrets and other assets. Depending on the rigidity or flexibility of the contractual tools in place, such updated, i.e., supplemental, modified or enhanced, tools may be necessary to accommodate, for example, ownership or license rights to modified, derived or jointly developed trade secrets or other assets, including tangible assets and other intellectual property. As a more specific example, negotiation or renegotiation of a residuals clause, or a ban or limitation on a party's future acquisition, access, disclosure and use of or to such trade secrets or other assets may be needed.

Also of note are the broader issues of compliance with contractual obligations and exercising contractual rights as the relationship evolves. For example, there may be an increase, a plateau or decrease of trade secrets being shared, with each such scenario presenting the parties an opportunity to assess whether obligations have been met and are still applicable and adequate, i.e., whether they need to be updated to account for changed circumstances, and whether rights have been timely and properly exercised and are still adequate. Such obligations may include sales reporting and royalty payment obligations for commercial use or embodiments of a trade secret. Such rights may include audit and inspection rights. Those rights may include the right to audit which personnel, such as key individuals, are still, no longer or newly involved in the relationship and if not, why and if so, how. Also, use of a third-party neutral to assess compliance with one or more obligations may be an appropriate process for the parties to consider and include in their relationship at a certain point, if such a process was not initially or is not yet part of their relationship. Likewise, it may become necessary to update the physical and technological tools to protect shared and other trade secrets, i.e., any modified, derived or jointly developed trade secrets.

Common physical tools, as discussed above in Section IV.C.2, control access to the shared trade secrets. A notable example of such a tool is a data room for evaluating shared trade secrets. Examples of related technological tools are software to log who accesses a physical data room, such as with a key card or biometric information, and software to log who accesses ESI through a device in that room or through a device that provides access to a virtual data room. Updating such physical and technological tools often depends on an assessment of the personnel accessing the data room and the cards, information and devices being used to gain access to the data room and trade secrets.

Typical inquiries include whether such devices are authorized, accounted for, being used properly and running current versions of software. Issues that may be identified include unauthorized downloading, uploading, copying, attaching, saving or printing of trade secrets. Such activities would likely result in updating corresponding physical and technological tools to meet the agreed level of protection and possibly result in taking other steps to protect and enforce respective interests and rights.

VI. CONSIDERATIONS WHEN ENDING DUE DILIGENCE OR A RELATIONSHIP

When due diligence or a relationship ends, measures to protect the confidentiality and thus, the status and value of a shared trade secret are typically taken. Some of those measures may continue beyond the due diligence or relationship and some may be supplemental, modified or enhanced measures that commence when the due diligence or relationship ends. Those measures may be set forth in an NDA or other contract between the disclosing party and receiving party. Generally, both parties will have protective measures obligations, with the disclosing party often focused on the receiving party's compliance with its obligations. That focus often includes the disclosing party seeking confirmation, in action and writing, that the receiving party has met and will continue to meet its obligations. For example, and as discussed above, the disclosing party often will expect and seek (1) return or destruction of the shared trade secrets in the receiving party's possession and (2) the receiving party's written confirmation that those obligations have been fulfilled. A receiving party also often has one or more continuing obligations, such as an obligation to maintain the confidentiality of the trade secrets it received and an obligation to refrain from accessing, reviewing, disclosing or using them. That obligation can be part of a belt and suspenders approach that accounts for the possibility of the receiving party breaching or otherwise failing to comply with the return or destruction obligation, whether by refusal, deficiency, mistake or otherwise.

Depending on how the trade secrets were shared and the obligations specified in the NDA or other contract, a disclosing party may also expect and seek written verification that: (1) any devices, platforms, databases or repositories, which the disclosing party provided or to which the disclosing party provided access, are returned or disabled, (2) any information, which the disclosing party provided or to which the disclosing party provided access and which was or is stored on any device the receiving party will continue to possess is deleted and (3) the receiving party reminds its team members and others involved in the trade secret sharing of confidentiality obligations. Permanent deletion of trade secrets may be achievable, especially if the receiving party adhered to obligations regarding, i.e., limitations on, storage, acquisition, access, review, disclosure, and use of or to the trade secrets. At the same time, the parties may agree that the receiving party can maintain in confidence and securely store archival copies that can be acquired, accessed, reviewed, disclosed, or used only during or in specific circumstances, such as a dispute concerning the trade secrets. Those archival copies may be maintained by and stored with, for example, an outside attorney, an in-house legal department, or an approved third party.

A disclosing party should account for any written materials, physical materials, such as a prototype or model, and digital or physical credentials, such as usernames, passwords, key cards or badges, that were provided to the receiving party and ensure they are returned, destroyed or disabled. To bolster protective measures and possibly motivate compliance and reduce the risk of a breach or other failure by the receiving party, whether by refusal, deficiency, mistake or otherwise, a disclosing party also can provide written reminders to the receiving party of its continuing obligations, including confidentiality obligations. A disclosing party also can compare the most current list, or inventory, of disclosed trade secrets to a list, or inventory, of returned or destroyed trade secrets to further those

same purposes.[53] This comparison can be quite important, as it objectively determines which trade secrets may be at risk, or at a higher risk, of misappropriation. Depending on the terms of the NDA or other contract, other measures, such as interviewing receiving party personnel about awareness of and compliance with obligations and potential risks, also can be taken. Notably, such measures are an example of measures that may be seen as not commercially feasible or reasonable, especially by the receiving party. Indeed, such a viewpoint may exist when the NDA or other contract is being negotiated or when the disclosing party requests such measures without a contractual basis for doing so.

Because of the prevalence of ESI, human error and sometimes even bad intent, the return or destruction of all relevant information may not be possible. But as noted above, a disclosing party can still compare the trade-secret inventories and, if necessary and accounted for in the NDA or other contract, inventory and examine relevant devices, including forensically. Devices that can store trade secrets include smart phones, computers, whether a desktop, laptop or tablet, external storage or memory devices and any online accounts provided to or accessed or used by the receiving party. Whether a given device is or was an authorized device is also an important issue. As such, timely preparing and updating an inventory of authorized devices is a step the disclosing party can take, preferably in cooperation with the receiving party, to assist in the return or destruction process. The disclosing party can also compare the returned information to the tracked history of the receiving party's information access and, as appropriate, act upon any discrepancy.

The above measures, along with the discussion below, provide a framework for a disclosing party to protect its trade secrets when and after a due diligence or relationship ends, whether by its own terms or by termination. A receiving party can also consider this framework as a possible means to facilitate its compliance with obligations and reduce its risk of committing trade secret misappropriation or breaching an NDA or other contract.

As noted above, an NDA, like any contract, may not address every issue that arises. In other words, circumstances can be overlooked or unforeseen during a contracting process. Nevertheless, many parties can negotiate and agree to provisions that will provide more certainty and better protection—for the trade secrets and the parties—when ending the due diligence, as always happens, or ending the relationship, as often happens. Below, we discuss several issues of which parties should be aware when ending due diligence or a relationship and potential ways to address those issues.

---

[53] The information set forth in both lists should be enough for the list to serve its purpose, with the disclosing party or both parties evaluating the scope of information and level of detail according to the contractual terms of their relationship.

Principle No. 9: The ending of due diligence or a relationship where trade secrets were shared is an opportunity for the parties to confirm, in writing, the status of the sharing, including the trade secrets that were shared and the receiving party's return or destruction of the shared trade secrets and other materials, such as documents identifying or embodiments of the shared trade secrets.

A. Failure to Update and Finalize Identification and a List of Trade Secrets Shared, Modified or Jointly Developed

A disclosing party is responsible for knowing what its trade secrets are, properly identifying and listing them, and updating and finalizing such efforts when sharing them with a receiving party. Thus, at or near the conclusion of due diligence or a relationship, the disclosing party should know what trade secrets were shared and be prepared to confirm that sharing, in writing, with the receiving party. In other words, this confirmation process, which can be set forth in an NDA or another contract between the parties, is an opportunity to align the parties' understandings regarding the trade secrets shared and any rights and obligations relating thereto.

There may be a legitimate, objective dispute about what trade secrets were shared or the parties' current situation may not be amicable, and communication may not be timely, clear or sufficient. One way to potentially avoid or limit those or similar circumstances is for the NDA or other contract to set forth a process for providing or obtaining confirmation or clarification of the identification or list of the shared trade secrets. Such a process could be in effect throughout the trade secret-sharing process. If it is, then the process might encourage greater attention to detail by each party and might lead to more productive communication, whether the parties' situation is amicable or not. Whether such a process is in place or not, when the identification or list of shared trade secrets is or may be open to interpretation, either party can proactively confirm or clarify or seek confirmation or clarification of the identification or list of the shared trade secrets. If any such effort is made, it can, ideally, be made in writing. Such effort can reduce the risk of and perhaps eliminate a future dispute, or at least reveal a current dispute.

Such a process is not without potential pitfalls. If the receiving party does not seek confirmation or clarification and a future dispute arises, such a failure may expose the receiving party to corresponding liability, or greater liability, or waive or otherwise negatively impact its rights or defenses.[54] Depending on the terms of the process, the disclosing party may or may not be obligated to confirm or clarify the identification or list of the shared trade secrets upon request of the receiving party. But the failure to do so may waive or otherwise negatively impact the disclosing party's attempt to subsequently do so in litigation.

Also worth mentioning is a late request for confirmation or clarification where a process for doing so is not set forth in the NDA or other agreement. That is, if the receiving party makes such a

---

[54] Convolve, Inc. v. Compaq Computer Corp., 527 Fed. Appx. 910 (FED. CIR. 2013) (failing to comply with NDA's written follow-up memoranda requirements waived party's rights under the NDA).

request at the end or nearly the end of the parties' relationship, then it may trigger scrutiny from the disclosing party, result in greater overall uncertainty for the receiving party and, in the event of litigation, a stronger argument from the disclosing party that the receiving party waived or limited its rights or defenses. This situation especially illustrates the potential benefits of greater attention to detail during the trade-secret-sharing process and, where appropriate, timely requests for confirmation or clarification pursuant to an NDA or other agreement or even in the absence of an express contractual provision.

A trade secret may be deliberately modified during the parties' due diligence or relationship. In other words, the trade secret may be modified not because of a deficiency or error, but to account for a different component, input, interface or application, for example. Three issues immediately can arise, and those issues can be addressed in the NDA or another agreement between the parties. First, are the modifications—including who made the modification, the date of the modification and other pertinent details—properly and timely documented? Second, who owns the stand-alone modification, i.e., potential trade secret, and corresponding rights and interests? Third, who owns the modified trade secret, i.e., the original trade secret plus the modification, and corresponding rights and interests?

Finally, the parties may be in a joint venture or other joint development-based relationship, or joint development may occur as the parties' relationship progresses or evolves. The parties, through their efforts, may jointly develop assets, including potential trade secrets, and one or both parties may then derive assets from a jointly developed asset. Like the circumstances where a modified trade secret is at issue, three issues immediately can arise, and those issues can be addressed in the NDA or another agreement between the parties. First, is the joint development work—including who performed the work, the date of the work and other pertinent details—properly and timely documented? Second, who owns the jointly developed asset and corresponding rights and interests, including the rights and interests in any derivative assets? Third, if only one party owns the jointly developed asset and corresponding rights and interests, does the other party retain or receive any rights or interests, such as a non-exclusive right or license to use the jointly developed asset?

B. Trade Secrets Not Returned or Destroyed When Due Diligence or a Relationship Ends

The parties' NDA or other contract can include a provision obligating the receiving party (1) to return or destroy all the trade secrets it received, (2) to do so upon the disclosing party's written request or fulfillment of another condition, such as the ending of the parties' due diligence or relationship, (3) to do so by a certain deadline, and (4) to confirm, in writing, to the disclosing party that all such trade secrets have been return or destroyed. In many situations, the receiving party can satisfy those obligations. Indeed, with notice of those obligations in an NDA, i.e., before any trade secrets are shared, the receiving party can take steps to ensure its means and scope of acquisition, access, review, disclosure, and use of the shared trade secrets will not interfere with—and will facilitate—those obligations.

Even with those obligations in place, a receiving party may fail to return or destroy all received trade secrets when due diligence or a relationship ends. Such a failure may result, for example, from (1) a receiving party's deliberate decision not to comply with the return or destruction obligation, (2) a receiving party's lack of technical acumen or ability, (3) a receiving party's difficulty in accounting for, or overlooking, trade secrets routinely backed up or archived and stored in memory the receiving party routinely uses to back up or archive its information, at least temporarily, (4) inability to remove notes or information regarding trade secrets from internal notes or materials, or (5) human error. Such a failure may lead to a dispute between the parties and constitute, for example, trade-secret misappropriation or a breach of contract, especially if the parties do not account for the failure in the NDA or another contract and the backed-up or archived trade secrets are not maintained in confidence.

The parties' NDA or other contract can address the possibility of the above failures by, for example, (1) obligating the receiving party to (a) confirm that the backed-up or archived trade secrets are destroyed, or permanently deleted, in the normal course of the receiving party's document retention or other applicable policy or (b) implement a specific technical solution, if feasible, and (2) specifying cure procedures and remedies for any breach of those obligations.

The parties can include a provision requiring the receiving party to explain, in writing, to the disclosing party any asserted justification for any non-return or non-destruction of a trade secret, including that return or destruction conflicts with a litigation hold, a trade secret is embedded in an attorney-client communication and part of a corresponding attorney-client privilege claim, or a trade secret is embedded in work product and part of a corresponding work product protection claim. Such an explanation may facilitate a solution, even if delayed, and may reduce the risk of a dispute that leads to litigation.[55] The parties can also include a provision authorizing the receiving party to securely archive copies of shared trade secrets. Such copies could be archived through, for example, a mutually approved third-party escrow service and be accessible to or used by the receiving party, i.e., its counsel or specific receiving-party personnel, only in the event of a future dispute between the disclosing party and receiving party.[56] The above-described process for the parties to confirm, in writing, what trade secrets have been shared can facilitate such archiving.

C. Subsequent Work Relating to Trade Secrets Is Performed by the Receiving Party or by Receiving Party Personnel Who Depart and Work Elsewhere

A potentially precarious situation exists where the receiving party engages in its own allegedly independent work relating to the trade secrets, the receiving party enters into a relationship with a third party where they engage in work relating to the trade secrets or receiving party personnel, such as employees, vendors, consultants and independent contractors, who acquired, accessed, reviewed,

---

55 As a practical matter, a receiving party with experience implementing and releasing a litigation hold may be able to apply that experience to comply with its return or destruction obligations.

56 The disclosing party's access to and use of the archived copies of shared trade secrets, i.e., its trade secrets, can justifiably not be so limited.

disclosed or used the trade secrets, take a new job or role where the new employer or partner is engaging in work relating to the trade secrets.

Four issues immediately can arise: (1) whether the receiving party returned or destroyed all the trade secrets, (2) whether the receiving party confirmed that it returned or destroyed all the trade secrets, (3) whether actual trade secret misappropriation, through unauthorized acquisition, disclosure or use, is taking place, and (4) whether trade secret misappropriation, through unauthorized acquisition, disclosure or use, is threatened, including whether such misappropriation is inevitable.[57]

As discussed above, establishing and maintaining trade secret status for information requires that the information be the subject of reasonable protective measures. That obligation typically is tied to the circumstances. Thus, where the circumstances change as described above, the protective measures may need to be supplemented, modified or enhanced. A first step to reasonably supplementing, modifying or enhancing those protective measures may be to promptly notify the receiving party, in writing, of the circumstances and concerns and request confirmation, or re-confirmation, that the receiving party has returned or destroyed all the shared trade secrets and has complied and is complying with all other obligations, including non-use and non-disclosure obligations. A next step, which may be or include initiating litigation, will likely be driven by the receiving party's response or non-response.

As also discussed above, the parties may have accounted for some or all of the foregoing circumstances in a pre-litigation dispute provision in an NDA or another contract. The parties also may have specified, in one or more contracts, permissible and impermissible work or other activity, including new or expanded business relationships, after due diligence or the relationship ends, with such provisions addressing, for example, covered subject matter, walling off receiving-party personnel and the duration of any restrictions.

---

[57] Inevitable misappropriation is a viable claim in some jurisdictions, but not in others, and is also a claim that can be asserted against an individual or entity. *See* Pelletier, Dean, "Never Out Of Style: Properly Tailored Inevitable Misappropriation Claims And Contractual Provisions," p. 1 n.2 (July 21, 2022), first presented at Practising Law Institute conference, Advanced Trade Secrets 2022: New Risks, New Challenges, New Ideas (Oct. 12, 2022) ("For example, Illinois and Pennsylvania are two of several jurisdictions that recognize inevitable misappropriation as a form of threatened misappropriation and, as such, as a basis for relief. *See, e.g.,* PepsiCo, Inc. v. Redmond*,* 54 F.3d 1262 (7th Cir. 1995) *and* Certainteed Ceilings Corp. v. Aiken, Civil Action No. 14-3925, at *4 (E.D. Pa. Jan. 29, 2015). *See also* Kinship Partners, Inc. v. Embark Veterinary, Inc., 3:21-cv-01631-HZ, at *13 (D. Or. Jan. 3, 2022) ('Several states recognize the inevitable disclosure [*sic*, misappropriation] doctrine under their respective trade secret misappropriation statutes.') (internal citation omitted); *and id.* ('Seventeen states appear to have adopted the inevitable disclosure [*sic*, misappropriation] doctrine in one form or another.') (internal citation omitted). California, Colorado, Louisiana, Maryland, Oregon, Virginia and the District of Columbia do not recognize—and, in some cases, have 'specifically rejected'—inevitable misappropriation as a form of threatened misappropriation and, as such, as a basis for relief. *Certainteed*, at *4; *and Kinship,* at *13 n.3. As to federal law, the consensus is the DTSA, which expressly provides relief for any actual or threatened misappropriation, does not encompass or provide relief for inevitable misappropriation by an individual. *See* 18 U.S.C. § 1836(b)(3)(A)(i)(I), (II).")*, and id.* at 12–13.

D. Receiving Party or Receiving Party Personnel Are Pursuing, Later Pursue or Enter Relationship with a Competitor of Disclosing Party

Two of the precarious situations addressed above can become riskier where a third-party competitor of the disclosing party is involved. That is, where (1) the receiving party is pursuing, later pursues, or enters into a relationship with a competitor of the disclosing party and they engage in work relating to the trade secrets, or (2) receiving party personnel such as employees, contractors, vendors, consultants and independent contractors who acquired, accessed, reviewed, disclosed or used the trade secrets, take a new job or role where the new employer or partner is a competitor of the disclosing party and engaging in work relating to the trade secrets, the risk of unauthorized acquisition, disclosure or use of the trade secrets can increase. These situations may become more complicated if the competitor of the disclosing party denies that the claimed trade secrets are entitled to trade secret protection. An NDA or other contract can address these circumstances, bearing in mind that contractual restrictions or prohibitions on an entity's activity or relationships can be distinct from and more easily enforced than contractual restrictions or prohibitions on an individual's activity or relationships, such as new employment or other roles.

E. Receiving Party Hires or Retains Disclosing Party's Present or Former Personnel

Another potentially precarious situation is where disclosing party personnel, such as a present or former employee, is hired by the receiving party after due diligence or a relationship between the disclosing party and receiving party ends. Such hiring poses a risk that the former disclosing party employee will perform work for the receiving party that involves trade secret misappropriation, i.e., actual or threatened, including inevitable, disclosure or use of one or more of the disclosing party's trade secrets. Importantly, the trade secrets at issue may include trade secrets the disclosing party shared with the receiving party and trade secrets the disclosing party did not share with the receiving party. A first step for the disclosing party may be to notify the receiving party, in writing, of the circumstances and concerns and request confirmation, or re-confirmation, that the receiving party has complied and is complying with all applicable obligations and, to the receiving party's knowledge, the former employee has and is as well. A next step, which may be or include initiating litigation, will likely be driven by the receiving party's response or non-response.

The parties may have accounted for the foregoing circumstances in a pre-litigation dispute provision in an NDA or another contract. The parties also may have specified, in an NDA or another contract, permissible and impermissible solicitation, recruitment, interviewing and hiring practices involving current and former personnel, including employees. Whether non-solicit, non-recruit or noncompete provisions or other employment-related restrictions are enforceable largely depends on the jurisdiction. Recent developments relating to noncompetes, including the increasing number of states banning or limiting noncompetes and agreements that have a similar effect, necessitate that confidentiality, including non-disclosure, obligations are properly focused on protecting the trade secrets and other protectible interests at issue.

A receiving party can mitigate the risks described above by designing and implementing an onboarding, including interviewing, process that includes, for example: (1) obtaining and reviewing a copy of any non-confidential restrictive covenant into which the new employee has previously entered and, as permitted, obtaining and reviewing a copy of any confidential restrictive covenant into which the new employee has previously entered; (2) obtaining from the new employee a signed, written verification that (a) the new employee is not violating and will not violate an obligation to a former employer by accepting and undertaking the new employment, (b) the new employee has fully complied with all return and destruction obligations (e.g., regarding any device, trade secret or other information) of the former employer and (c) the new employee does not possess, on any device or in any tangible (e.g., paper or electronic) form, any trade secret or other confidential, secret or proprietary information of the former employer; (3) establishing, in writing, the new employee's obligations to the new employer, including not to acquire, access, disclose or use any trade secrets, or other confidential, secret or proprietary information, of the former employer; (4) ensuring the new employee is educated on confidentiality, including the new employer's corresponding policies and procedures; (5) obtaining an executed confidentiality agreement between the new employer and new employee; (6) maintaining a completed, signed onboarding checklist in the new employee's file; and (7) ensuring the new employee is not performing and does not perform work that involves, or unreasonably risks involving actual or threatened, including inevitable, disclosure or use of the former employer's trade secrets.[58] All the above steps might not be possible, or might not be performed in a particular company setting. Relatedly, differences in applicable law can inform or modify aspects of an onboarding process. But where a receiving party hires a disclosing party's personnel, such as a present or former employee, the receiving party can balance its resources with the opportunity and need to protect itself.[59]

F. Considerations when Sharing Trade Secrets Internationally

International sharing of trade secrets raises unique issues when due diligence or a relationship ends.[60] As an initial matter, proper identification of trade secrets is particularly important where trade secrets are shared internationally, as enforcement can be especially difficult without proper identification. Further, given the rise of economic espionage in an increasingly globalized, digital business world with more frequent cross-border sharing of trade secrets, disclosing parties often need a systematic approach to protect their trade secrets and promptly enforce them. Of course, the approach will differ depending on the disclosing party, its resources, the receiving party and the country or countries at issue.

---

58 The above discussion expressly addresses employees and employers. It also can apply to other relationships involving other personnel, such as vendors, consultants and independent contractors.

59 The Sedona Conference, *Commentary on Protecting Trade Secrets Throughout the Employment Life Cycle*, 23 SEDONA CONF. J. 807 (2022), *available at* https://thesedonaconference.org/, substantively analyzes, for example, trade secret considerations that can arise in connection with employees.

60 For in depth-analysis regarding issues related to international sharing of trade secrets, *see* The Sedona Conference, *Framework for Analysis on Trade Secret Issues Across International Borders*, 23 SEDONA CONF. J. 909 (2022).

Despite those unique issues, where a disclosing party intends to share trade secrets with a foreign receiving party, the disclosing party can proceed by accounting for the same or similar issues it accounts for when sharing trade secrets with a domestic receiving party. The disclosing party's focus would be protecting its trade secrets, anticipating and preparing for litigation to enforce its rights and considering the following:

a. Discovery is less available for litigation in international forums,[61] so consider being vigilant in tracking, documenting, and managing any documents and activity relating to sharing trade secrets in case a dispute arises.

b. Take steps set forth in Section IV(B) to the extent available and applicable to trade secrets disclosed to a foreign receiving party.

c. Pursuant to a contract with the receiving party, consider memorializing the identification and a list of the shared trade secrets at an appropriate time, to an appropriate degree, and in an appropriate manner.

d. Consider documenting the return and destruction of trade secrets by the receiving party.

e. Pursuant to a contract with the receiving party, consider memorializing ownership, retention, and other rights and interests in and to any modified or jointly developed trade secrets.

f. Ensure compliance with applicable data protection or transfer laws.

g. To the extent the disclosing party discovers or believes that trade secrets were or are being misappropriated during due diligence or the relationship, but the disclosing party still wants or needs services of the receiving party because of, for example, business reasons, consider a strategy to document and effectuate the disassociation of the parties. The strategy would seek to limit and, if possible, eliminate through contractual, physical and technological tools, the receiving party's current and future acquisition, access, review, disclosure, and use of the trade secrets, while ensuring sufficient time and opportunity to comply with applicable statutes of limitation for a trade secret misappropriation or other action.[62]

h. Consider choice of law and potential forums and venues for any dispute. As discussed in Section IV.C.1 above, parties can include choice of law and forum and

---

61 For additional guidance *see* The Sedona Conference, *Commentary on Cross-Border Discovery in U.S. Patent and Trade Secret Cases ("Stage Two")*, 24 SEDONA CONF. J. 549 (2023).

62 Ping-Hsun Chen, TRADE SECRET PROTECTION AGAINST MISAPPROPRIATION COMMITTED BY YOUR FOREIGN DISTRIBUTOR-A LESSON FROM ATRICURE, INC. V. JIAN MENG, 102 J. Pat. & Trademark Off. Soc'y 252, 263 (2022).

venue selection provisions in an NDA or another contract. International trade secret sharing can elevate the importance of those provisions. The different potential forums for disputes have various costs and benefits for the disclosing party and receiving party.[63]

i. Regarding points a and h above, U.S. Courts increasingly offer a relatively favorable environment for companies to pursue trade secret misappropriation claims against foreign defendants. U.S. Courts interpreting both the DTSA and some States' versions of the UTSA are permitting extraterritorial misappropriation claims.[64] But given the difficulty in obtaining foreign discovery, especially in a U.S. district court or State court action, potential personal jurisdiction issues and enforcing any remedy, disclosing parties, i.e., potential plaintiffs, need to be well organized in collecting evidence for such claims prior to, during, and after exiting due diligence or a relationship involving sharing trade secrets with a foreign receiving party.

j. Regarding points a and h above, the U.S. International Trade Commission likewise offers a relatively favorable environment for companies to pursue trade secret misappropriation claims against foreign respondents.

---

63 For in depth-analysis of issues relating to the forums and legal regimes chosen for disputes over internationally shared trade secrets, including various U.S. State Courts, U.S. District Courts, the U.S. International Trade Commission, the Economic Espionage Act of 1996, regulatory actions and the World Trade Organization's Agreement on Trade-Related Aspects of Intellectual Property Rights, *see* The Sedona Conference, Framework for Analysis on Trade Secret Issues Across International Borders, 23 SEDONA CONF. J. 909 (2022).

64 *See, e.g.,* DTSA, 18 U.S.C. § 1837; vPersonalize Inc. v. Magnetize Consultants Ltd.*,* 437 F. Supp. 3d 860, 878–79 (W.D. Wash. 2020) (stating that "18 U.S.C. § 1837 authorizes civil enforcement actions against foreign entities to the same extent as criminal actions" and collecting cases); Motorola Sols., Inc. v. Hytera Commc'ns Corp.*,* 436 F. Supp. 3d 1150, 1165 (N.D. Ill. 2020) ("the Court holds that the DTSA may apply extraterritorially in this case because the [act in furtherance] requirement of [18 U.S.C. § 1837(2)] has been met")*,* Motorola Sols., Inc. v. Hytera Commc'ns Corp.*,* 108 F.4th 458, 488 (7th Cir. 2024) (*rev'd in part, aff'd in pertinent part and remanded*) *and* Motorola Sols., Inc. v. Hytera Commc'ns Corp.*,* 2024 WL 4416886 (7th Cir. 2024) (petition for rehearing *en banc* denied); AtriCure, Inc. v. Jian Meng*,* 842 F. App'x 974, 983 (6th Cir. 2021) (holding the Ohio UTSA applies extraterritorially against Chinese defendants concerning conduct in China); *and* Miller UK Ltd. v. Caterpillar Inc., No. 10-CV-03770, 2017 WL 1196963, at *7 (N.D. Ill. Mar. 31, 2017) (concluding the Illinois Trade Secrets Act (ITSA) has extraterritorial effect because the ITSA specifically states that "a contractual or other duty to maintain secrecy or limit use of a trade secret shall not be deemed to be void or unenforceable solely for lack of durational or geographical limitation on the duty.").

VII. APPENDIX

Parties can consider the following points before and when sharing trade secrets.

Disclosing Party

- What is the fewest number of trade secrets that can be shared to satisfy the purpose?
- Can the disclosure consist of physical documents or electronic files that can be marked and traced?
- What is the fewest number of individuals who need access to, i.e., need to know, the shared trade secrets?
- Can any such access be limited in time, by device or access point, by purpose or otherwise?
- What are the tools the disclosing party uses to protect its trade secrets?
- What are the tools, including supplemental, modified, or enhanced tools, the receiving party needs to use to protect the trade secrets?
- Is an NDA or other agreement in place? If so, are the following provisions in effect or needed:
- Identification of trade secrets
- Marking requirement, including in connection with oral disclosures
- Authorized and unauthorized individuals (or titles)
- Modification of, derivation from and joint development of trade secrets and other assets
- Legal and regulatory obligations, including disclosures and corresponding cooperation
- Ending of due diligence or relationship, including return or destruction obligations
- Milestone events in NDA or other agreement, including results or consequences
- Audit, inspection and examination rights
- Reverse engineering prohibition
- Is another contractual tool, such as a noncompete, in place or a necessary and available option?
- What are the technological tools to be used by the receiving party to protect the trade secrets?
- What are the physical tools to be used by the receiving party to protect the trade secrets?
- Will there be international sharing of the trade secrets? If so, are there corresponding laws or regulations to be taken into account?
- Are there applicable third-party obligations or issues?

Receiving party

- What is the fewest number of trade secrets that can be shared to satisfy the purpose?
- Can the disclosure consist of physical documents or electronic files that can be marked and traced?

- What is the fewest number of individuals who need access to, i.e., need to know, the shared trade secrets?
- Can any such access be limited in time, by device or access point, by purpose or otherwise?
- What are the tools the disclosing party uses to protect its trade secrets?
- What are the tools, including supplemental, modified or enhanced tools, the receiving party needs to use to protect the trade secrets?
- Is an NDA or other agreement in place? If so, are the following provisions in effect or needed:
- Identification of trade secrets
- Marking requirement, including in connection with oral disclosures
- Authorized and unauthorized individuals (or titles)
- Modification of, derivation from and joint development of trade secrets and other assets
- Residuals clause
- Feedback clause
- License
- Legal and regulatory obligations, including disclosures and corresponding cooperation
- Ending of due diligence or relationship, including return or destruction obligations
- Milestone events in NDA or other agreement, including results or consequences
- What are the technological tools to be used by the receiving party to protect the trade secrets?
- What are the physical tools to be used by the receiving party to protect the trade secrets?
- Is a non-exclusive right to evaluate or work in the area pertaining to the trade secrets needed?
- In a supply relationship, is an obligation to continue supplying for a period under reasonable terms needed?
- Will there be international sharing of the trade secrets? If so, are there corresponding laws or regulations to be considered?
- Are there applicable third-party obligations or issues?