

## Required Reading

1.1 – What Is or Is Not a Trade Secret –  
Project Charter/Draft Commentary, August  
31, 2022

**Brainstorming Group Outline/Project Charter**

**WG12 What Can and Cannot Be a Protectable Trade Secret?**

**August 31, 2022**

# ***Table of Contents***

---

<b><i>I. Introduction.....</i></b>	<b><i>1</i></b>
<b><i>II. What Can Be a Protectable Trade Secret? .....</i></b>	<b><i>3</i></b>
<b><i>A. Trade Secrets Generally and Specific Examples .....</i></b>	<b><i>3</i></b>
<b><i>B. Secrecy .....</i></b>	<b><i>4</i></b>
<b><i>C. Combination Trade Secrets .....</i></b>	<b><i>7</i></b>
<b><i>III. General Skill and Knowledge.....</i></b>	<b><i>9</i></b>
<b><i>IV. Confidential Information.....</i></b>	<b><i>12</i></b>
<b><i>A. Historical Context.....</i></b>	<b><i>12</i></b>
<b><i>B. Preemption of Other Remedies Related to Trade Secrets and Confidential Information.....</i></b>	<b><i>15</i></b>
<b><i>C. Enforceability of Contracts Covering Confidential Information .....</i></b>	<b><i>18</i></b>

## ***Proposed Principles “At a Glance”***

---

**[Proposed] Principle No. 1 – To determine whether information is a trade secret, parties should define the relevant audience from whom the information must be kept secret and determine the state of general knowledge in the field or industry. Expert testimony may be useful in this analysis.**

**[Proposed] Principle No. 2 – A combination of information, each element of which is publicly known, can be protectable as a trade secret if the unified combination meets the requirements to be a trade secret—namely, the combination is not generally known to or readily ascertainable by the relevant public (or those who can obtain value from it); has been the subject of reasonable measures to protect it; and provides actual or potential economic value because of secrecy.**

**[Proposed] Principle No. 3 – Determining whether information is properly classified as general skill and knowledge requires a careful balancing of facts and interests, and will necessarily be context specific.**

**[Proposed] Principle No. 4 – Employees and others may have a duty of confidentiality with respect to confidential information under legal regimes other than trade secrets law. Other causes of action, in particular contract law, may exist to enforce that duty or protect such confidential information in certain circumstances.**

**[Proposed] Principle No. 5 – Whether a legal claim related to confidential information is preempted by state trade secret law depends on many factors, including which version of the UTSA’s preemption provision the state has adopted and court decisions interpreting that provision, the nature of the information at issue, the legal regime on which the claim is based, especially whether it is a contract or a non-contract claim, the source of the duty on which the claim is based, and the conduct and factual circumstances giving rise to the claim, in particular whether there is wrongdoing that is separate from use or disclosure of confidential information.**

# ***I. Introduction***

---

Trade secrets are generally defined in both the Uniform Trade Secrets Act (“UTSA”) and the Defend Trade Secrets Act (“DTSA”) as information that derives “independent economic value” from not being “generally known” by others or “readily ascertainable” by others using “proper means” and which the owner has taken “reasonable measures” to keep secret. Although the UTSA was published more than thirty years ago, courts still diverge markedly over the precise contours of trade secret protection. This issue has been complicated by the digitization of information and the way in which parties develop, protect, and share valuable confidential information.

In this *Commentary*, Working Group 12 will provide guidance as to current approaches to defining what is and what is not a trade secret and the flashpoints for the areas in which the case law is likely to develop in the foreseeable future. This *Commentary* offers consensus recommendations where possible, and where the case law is still developing, ideas on how to conceptualize where the lines should be drawn.

In Part I of this *Commentary*, we discuss what a trade secret is and how companies, individuals, courts, and others should go about determining what is a trade secret. We cover the criterion that a trade secret be “not generally known” or “readily ascertainable” using “proper means.” We also discuss the unique case of protection for so-called “combination” secrets.

In Part II, we discuss the exclusion of what is commonly referred to as “general skill and knowledge.”<sup>1</sup> This excluded category originated in the common law and was intended to recognize the reality that employees will, and should be able to, gather information at one job and move to another. It is carried forward in the modern statutory regimes. However, the statutes provide very little guidance. Determining what falls into the excluded category of general skill and knowledge raises many difficult questions for courts and litigants that the *Commentary* will seek to address.

Finally, in Part III, we explore the scope of and protections for non-trade secret “confidential information” under other legal regimes, such as contract law or torts like conversion and breach of fiduciary duty. We discuss questions related to “preemption” (displacement) of claims related to trade secret law and various complications surrounding using contracts to protect confidential information that does not technically qualify as a trade secret.

---

<sup>1</sup> The phrase varies. In some instances it is expanded to “general skill, knowledge, training, and experience.” Regardless of the formulation, the concepts are the same. We will use the phrase “general skill and knowledge,” which is the formulation adopted by the Sedona Conference elsewhere. See The Sedona Conference, *Commentary on Protecting Trade Secrets throughout the Employment Life Cycle* (June 2021 public comment version), [https://thesedonaconference.org/sites/default/files/publications/Sedona%20WG12%20Employment%20Life%20Cycle%20%28June%202021%20publ%20comm%29\\_06-20-21.pdf](https://thesedonaconference.org/sites/default/files/publications/Sedona%20WG12%20Employment%20Life%20Cycle%20%28June%202021%20publ%20comm%29_06-20-21.pdf)

This *Commentary* does not address (a) issues surrounding the requirement of identification of trade secrets for moving forward with a trade secret misappropriation claim,<sup>2</sup> (b) forensic best practices for discovery of trade secrets in a proceeding, (c) the requirement of reasonable measures to maintain secrecy, (d) the requirement of independent economic value, as distinguished from the requirement of secrecy,<sup>3</sup> (e) extensive analysis of inevitable disclosure or threatened misappropriation,<sup>4</sup> (f) analysis of noncompetition law except as it relates to confidential information; or (g) broader topics of trade secret law, such as what constitutes misappropriation.

---

<sup>2</sup> This Commentary does not address issues surrounding the proper identification of trade secrets as opposed to substantive elements of trade secret protection and exclusions from protection. 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 CONFERENCE JOURNAL 223 (2021), available at: [https://thesedonaconference.org/publication/Commentary\\_on\\_Proper\\_Identification\\_of\\_Trade\\_Secrets\\_in\\_Misappropriation\\_Cases](https://thesedonaconference.org/publication/Commentary_on_Proper_Identification_of_Trade_Secrets_in_Misappropriation_Cases)

<sup>3</sup> For more details regarding managing trade secrets and guidelines for consideration in protecting trade secrets, see The Sedona Conference, Commentary on the Governance and Management of Trade Secrets (April 2022 public comment version), [https://thesedonaconference.org/sites/default/files/publications/Governance\\_and\\_Management\\_of\\_Trade\\_Secrets\\_public\\_comment\\_April\\_2022.pdf](https://thesedonaconference.org/sites/default/files/publications/Governance_and_Management_of_Trade_Secrets_public_comment_April_2022.pdf)

<sup>4</sup> For more details regarding identification of trade secrets issues, see The Sedona Conference, Commentary on Equitable Remedies in Trade Secret Litigation, 23 SEDONA CONFERENCE JOURNAL, No. 2 (2021).

(May 2021 public comment version), [https://thesedonaconference.org/sites/default/files/Sedona%20WG12%20Equitable%20Remedies%20%28May%202021%20publ%20comm%20over%29%20-%20Handout%20-%2005\\_03\\_21.pdf](https://thesedonaconference.org/sites/default/files/Sedona%20WG12%20Equitable%20Remedies%20%28May%202021%20publ%20comm%20over%29%20-%20Handout%20-%2005_03_21.pdf)

## ***II. What Can Be a Protectable Trade Secret?***

---

This part of the Commentary addresses what can be a protectable trade secret. It explores the types of “information” that can be protected under state and federal law, along with specific examples that may be of special relevance in today’s legal and business climate. It then addresses the major legal criterion of secrecy—that is, the requirement that information not be “generally known” or “readily ascertainable using proper means” to others. In addition, it addresses the special issues raised by so-called “combination” trade secrets.<sup>5</sup>

### **A. TRADE SECRETS GENERALLY AND SPECIFIC EXAMPLES**

The definition of “trade secret” is provided by both federal and state laws.

The Defend Trade Secrets Act (“DTSA”), effective as of May 11, 2016, provides, in relevant part, that a “ ‘trade secret’ means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing 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 by proper means by, another person who can obtain economic value from its disclosure or use the information[.]”<sup>6</sup>

This federal definition is expressly based on the Uniform Trade Secrets Act (“UTSA”), which was drafted in 1979 and which today serves as the basis for the trade secret statutes in most states.<sup>7</sup> There are differences between how the UTSA and the DTSA define “information.” However, the legislative history indicates the DTSA’s definition was not intended to be “meaningfully different from the scope of that definition as understood by courts in States that have adopted the UTSA.”<sup>8</sup>

**Key Issues for the Commentary to Address:** What types of “information” can potentially be protected under the DTSA and the UTSA? Are there important distinctions

---

<sup>5</sup> As noted above, this part does *not* cover related criteria, like whether information has been the subject of reasonable secrecy precautions or whether information derives sufficient economic value from secrecy.

<sup>6</sup> Defend Trade Secrets Act, 18 U.S.C. § 1839(3)(B) (2016).

<sup>7</sup> Uniform Trade Secrets Act, § 1(4) (as amended in 1985).

<sup>8</sup> *See, e.g.*, Senate Report No 114-220, at 10 (2016).

between the DTSA and the UTSA with regard to what information can be protected? What examples of trade secrets are most relevant to discuss today? Which types of trade secrets are likely to raise important law and policy issues? What complications are introduced by the digitization of information and the way in which parties develop, protect, and share valuable confidential information? What complications are introduced by changes in patent law—for instance, the determination that AI inventions that lack a human inventor cannot be patented and the ever-shifting patentability of business methods and inventions related to diagnostic methods and genetic information?

## **B. SECRECY**

Secrecy is the key to owning a protectable trade secret, but that secrecy need not be absolute. Instead, under federal law and the statutory regime adopted in most states, secrecy requires two things: that the information not be “generally known” to those “who can obtain economic value” from it; and that the information not be “readily ascertainable using proper means” to those other persons.<sup>9</sup> Each of these elements requires a deep understanding of the industry in order to determine whether information is sufficiently unknown to the relevant audience to be protectable.

### **1. Not Generally Known**

There are two main ways information can become generally known. First, it can be revealed in a publication or other public-facing disclosure, such as a journal article or a U.S. patent. Second, the information can become the common knowledge of so many people in the relevant industry that it is deemed generally known.<sup>10</sup> The primary evidence assessed in deciding what is generally known includes: publications and other disclosures; testimony from someone inside a plaintiff’s company; and testimony from either party’s proffered experts.<sup>11</sup>

The parties often disagree on the appropriate audience from whose perspective information’s secrecy is to be judged. A trade secret must not be generally known to the *relevant* persons, *i.e.*, those who can obtain economic value from the information. Clearly, that audience is not the general “public.” Indeed, the DTSA, as indicated in its legislative history, explicitly moved away from the “public” as the benchmark.<sup>12</sup> The UTSA

---

<sup>9</sup> The UTSA refers, in relevant part, to “*other persons* who can obtain economic value from its disclosure or use[.]” UTSA, § 1(4) (emphasis added). *See also* DTSA, 18 U.S.C. § 1839(3)(B) (2016) (using phrase “another person.”).

<sup>10</sup> *Catalyst*, 350 F. Supp. 2d at 9 (“[I]nformation which is ‘generally known within an industry,’ even if it is not generally known to the public, cannot constitute a trade secret.”) (quoting *Mangren Research & Dev. Corp. v. Nat’l Chem. Co.*, 87 F.3d 937, 942 (7th Cir.1996)).

<sup>11</sup> *See, e.g.*, *U.S. Gypsum Co. v. Lafarge N. Am. Inc.*, 670 F. Supp. 2d 748, 764 (N.D. Ill. 2009) (permitting defendant’s technical expert to “opine on what information constitutes a trade secret, based on what was known and generally available in the wallboard industry at the time in question.”)

<sup>12</sup> *See* S. Rep. No 114-220, at 10 (2016). The Economic Espionage Act had used “the public” to refer to the audience from whom information must be kept secret. This had been criticized in the courts. *See United States v. Lange*, 312 F.3d 263, 267 (7th Cir. 2002) (“A problem with using the general public as the reference



Commentary, for its part, had indicated that the relevant persons are the “principal persons” who might be able to obtain economic benefit from information and to whom the information might have some economic value. So, for example, information can be generally known and thus not protectable as a trade secret even if it is not publicly available—so long as people in the industry are aware of it.<sup>13</sup>

But beyond those general principles, it is often very difficult to identify who this audience is and what evidence is appropriate to consider. Another complication is that there are subtle differences in how the DTSA and the UTSA language define this audience. The DTSA refers to “another person” in the singular, whereas the UTSA uses the phrase “other persons” instead. The implications of this change have not been explored—though, as mentioned above, it seems unlikely that Congress intended the definitions to be meaningfully different.

Occasionally, courts have drawn analogies to the standards used to judge the novelty of an invention in patent law and the rules used for determining whether an old patent or printed publication counts as patent “prior art.” For example, in a trade secret and patent case, the Federal Circuit held that an alleged trade secret was legally public, and not protectable under California trade secret law, because it could be found in a Japanese patent. To justify this decision, the court cited to its own case law regarding what counts as patent prior art.<sup>14</sup> These two legal regimes are different, and the rules for judging the secrecy of a trade secret are not the same as those used to judge the novelty of an invention. It is worth considering how and why.

**Key Issues for the Commentary to Address:** How does one determine when information is “generally known? What types of evidence are relevant for this inquiry, and when should experts be used? From whom must information be kept secret—who are the UTSA’s “other persons who can obtain economic value” from the information, and who is the DTSA’s “another person who can obtain economic value” from the information? Non-trade secret lawyers often say that information is protectable if it is not “in the public domain” but “public domain” has a very different meaning under

---

group for identifying a trade secret is that many things unknown to the public at large are well known to engineers, scientists, and others ...”). So Congress changed the wording to “another person.”

<sup>13</sup> See UTSA, § 1 cmt. (“If the principal persons who can obtain economic benefit from information are aware of it, there is no trade secret.”). See also, e.g., *Altavion, Inc. v. Konica Minolta Sys. Lab., Inc.*, 226 Cal. App. 4<sup>th</sup> 26, 62, 171 Cal. Rptr. 3d 714, 743 (2014) (stating the issue as whether the information “is generally known to or readily ascertainable by business competitors or others to whom the information would have some economic value...”).

<sup>14</sup> The claimed trade secret related to the use of a combination of lithium carbonate and citric acid in calcium sulphoaluminate cement—it had been publicly disclosed in a Japanese patent. See *Ultimax Cement Mfg. Corp. v. CTS Cement Mfg. Corp.*, 587 F.3d 1339, 1355–56 (Fed. Cir. 2009) (applying California trade secret law) (“...Ultimax has not shown that it had a secret. Information disclosed in a patent, even a foreign one, is ‘generally known to the public,’ especially the relevant public in the cement industry. Indeed, one of the primary purposes of patent systems is to disclose inventions to the public.”) (citing to *Bruckelmyer v. Ground Heaters, Inc.*, 445 F.3d 1374, 1379 (Fed.Cir.2006), where the Federal Circuit had found a foreign patent, like a U.S. patent, counted as “prior art” because it was “publicly accessible” given that “one skilled in the art exercising reasonable diligence” could find it and it was “classified and indexed” in the foreign patent office).

Copyright Law than under trade secret law. How does the “not generally known” concept compare to patent law concepts like novelty and nonobviousness and how relevant are patent law determinations for what counts as “prior art” for purposes of obviousness and anticipation?

**[Proposed] Principle No. 1 – To determine whether information is a trade secret, parties should define the relevant audience from whom the information must be kept secret and determine the state of general knowledge in the field or industry. Expert testimony may be useful in this analysis.**

## **2. Not “Readily Ascertainable” Using “Proper Means”**

Under the DTSA and the laws of most states, trade secrets also do not include information that is “readily ascertainable through proper means by” other persons to whom it may impart economic value. Both the DTSA and the UTSA include this additional “readily ascertainable” language,<sup>15</sup> though not all states adopt this limitation.<sup>16</sup>

The not “readily ascertainable” language means that information is not a protectable trade secret, even if it is not public or generally known, when others could discern it “readily” and utilizing only “proper means.” Information may be deemed readily ascertainable using proper means, for example, if it is very easy to discern from inspecting a product sold on the open market or if it could theoretically be found in trade journals or reference books, even if it is not clear people have actually accessed them, so long as they could *potentially* do so without too much effort. But information that cannot be *readily* ascertained through *proper* means might still be protectable as a trade secret.

Needless to say, what is “readily” ascertainable can often be debated, as can, obviously, what counts as “proper” means” of ascertaining the information. Courts have enunciated strikingly different standards.<sup>17</sup> What is more, the digital age raises new complications. For instance, what if “the trade secret” is a database encompassing a vast collection of information that is not as a whole readily ascertainable, but computer “bots” can be used to “scrape” a substantial portion of the entire database faster than any human practicably

---

<sup>15</sup> 18 U.S.C. § 1839(3)(B) (2016); UTSA, § 1.

<sup>16</sup> California, for instance, does not. *See* Cal. Civil Code. 3426.1(d) (“‘Trade secret’ means information ... that ... [d]erives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use...”).

<sup>17</sup> *Compare* Flotec, Inc. v. S. Research, Inc., 16 F. Supp. 2d 992, 1000 (S.D. Ind. 1998) (“[T]rade secret law does not protect information that is publicly available, including information that can be discerned with reasonable effort by inspecting a product available for purchase on the market.”) *with* Art & Cook, Inc. v. Haber, 416 F. Supp. 3d 191, 196, 2017 U.S. Dist. LEXIS 164366, \*8-9, 2017 WL 4443549 (E.D.N.Y. October 3, 2017) (stating that the fact that compiling a list from public sources would be “an arduous task, involving ‘tens if not hundreds of hours’ of research is not alone sufficient to confer protection under the DTSA.”).

could? Does this information lose trade secrecy status, or is it in fact not “readily ascertainable” using “proper” means?<sup>18</sup>

**Key Issues for the Commentary to Address:** When is information readily ascertainable using proper means? How do we define “readily” and “proper” in this context? Who has the burden on these issues? Does it matter that information could theoretically have been readily ascertained using proper means by third parties, if defendant itself did not do so (for instance hiring one of plaintiff’s employees to obtain the information)? When might protections such as an agreement not to reverse engineer publicly available products stand as a barrier to entry for would-be competitors—can such anti-reverse engineering clauses transform otherwise readily ascertainable information into trade secrets? What is the interplay between the “not readily ascertainable” limitation and the well-accepted rule that trade secrets can be lawfully “reverse engineered”? Is the question of what is “readily ascertainable” just a policy determination that something should not be protected, or can a meaningful line be drawn?

### C. COMBINATION TRADE SECRETS

In cases involving so-called “combination secrets”—information that consists of a combination of otherwise-public information—many courts across jurisdictions apply what appear to be special rules, indicating in various ways that the combination *as a whole* must impart sufficient economic value due to secrecy to provide an actual or potential economic advantage over others. Courts sometimes refer to “combination trade secrets” in relation to “compilations,” which are mentioned in the statutes as being protectable.<sup>19</sup>

Different courts and jurisdictions provide a wide variety of iterations of how to frame this principle, using diverse conceptualizations of what is required to turn a compilation of publicly known elements into a protectable trade secret. For example, some courts have indicated that a “trade secret can exist in a combination of characteristics and components, each of which, by itself, is in the public domain, *but the unified process,*

---

<sup>18</sup> See *Compulife Software Inc. v. Newman*, 959 F.3d 1288, 1299, 1315-1316 (11<sup>th</sup> Cir 2020) (addressing whether accessing large amounts of a data constituting a compilation of individual insurance quotes from plaintiff’s website by hiring a “hacker” to “scrape” data from the server using a robot, i.e. a “bot,” constituted trade secret misappropriation, indicating that “the simple fact that the quotes taken were publicly available does not automatically resolve the question in the defendants’ favor[.]” though expressing no opinion as to whether “the means were improper such that the acquisition or use of the quotes could amount to misappropriation.”). Compare *CouponCabin, Inc. v. PriceTrace, LLC*, 2019 U.S. Dist. LEXIS 62438, \*8-9, 2019 WL 1572448 (N.D. Ill. 2019) (finding that coupon codes that were “imbedded in [plaintiff’s] website” were “available to the public” and not protectable under trade secret law, because “no subscription or user fee [was] necessary to access the coupon codes[.]” and the codes could thus potentially be discerned).

<sup>19</sup> DTSA, § 1839 (3); UTSA § 1(4). See also, e.g., *Prysmian Cables & Sys. USA, LLC v. Szymanski*, 573 F. Supp. 3d 1021, 1037 (D.S.C. 2021) (“[A] trade secret may exist in a unique combination or compilation of information otherwise publicly available. However, such a compilation trade secret must be sufficiently identified to provide reasonable details concerning the information which makes up the secret and how that information relates together to form the secret.”) (citations omitted).

*design and operation of which, in unique combination, affords a competitive advantage and is a protectable secret.”*<sup>20</sup>

Other courts use modifiers like “novel” and “unique” to describe what can be protected as a compilation, risking the potential interpretation that novelty in the patent sense is required or that the combination secrets somehow afford the owner exclusive or unique rights in information others may independently develop. To give just one example, the Eighth Circuit has stated that “a novel or unique combination of elements can potentially constitute a trade secret,” but that “mere variations on widely used [information] cannot be trade secrets.”<sup>21</sup> Still other courts are more holistic in their terminology. For example, a district court in the District of Columbia, in a patent and trade secret case that was affirmed by the Federal Circuit, has stated that “a trade secret can exist in a combination of characteristics ... each of which, by itself, is in the public domain ... only when there is an added value to the combination over the value of the individual parameters, i.e., when the whole is more than the sum of the parts.”<sup>22</sup> Yet other decisions appear to suggest, incorrectly, that if each element is generally known then a combination can never be a trade secret or require an explanation for the “connections” between pieces of publicly known information.

**Key Issues for the Commentary to Address:** What are common types of combination secrets? When does protection for combinations of information that is, individually, publicly known raise potential problems for law and policy? How do we decide when a combination of public information meets the definition of a trade secret? Which of the variety of rules and approaches taken by courts make the most sense as a matter of law and policy? Can we distill clearer or more accurate rules from the catch phrases that courts tend to use? Do combination secrets differ from “compilations,” mentioned in the statutes?

**[Proposed] Principle No. 2 – A combination of information, each element of which is publicly known, can be protectable as a trade secret if the unified combination meets the requirements to be a trade secret—namely, the combination is not generally known to or readily ascertainable by the relevant public (or those who can obtain value from it); has been the subject**

---

<sup>20</sup> See, e.g., *Anaconda Co. v. Metric Tool & Die Co.*, 485 F. Supp. 410, 422 (E.D. Pa. 1980) (quoting *Imperial Chem. Indus., Ltd. v. Nat'l Distillers and Chem. Corp.*, 342 F.2d 737, 742 (2d Cir. 1965)) (emphasis added); *Giasson Aerospace Sci., Inc. v. RCO Eng'g, Inc.*, 680 F. Supp. 2d 830, 841–42 (E.D. Mich. 2010) (“A trade secret can exist in a combination of characteristics and components, each of which, by itself, is in the public domain, but the unified process, design and operation of which, in unique combination, affords a competitive advantage and is a protectable secret.”) (citing *3M v. Pribyl*, 259 F.3d 587, 595–97 (7th Cir.2001)).

<sup>21</sup> *Strategic Directions Grp., Inc. v. Bristol-Myers Squibb Co.*, 293 F.3d 1062, 1065 (8th Cir. 2002) (affirming a lower court’s finding that a compilation of market research questions was not a trade secret) (applying Minnesota UTSA).

<sup>22</sup> See *Catalyst & Chem. Servs., Inc. v. Global Ground Support*, 350 F. Supp. 2d 1, 8-10 (D.D.C. 2004), *aff'd*, 173 Fed. Appx. 825 (Fed Cir. 2006) (citations omitted).

**of reasonable measures to protect it; and provides actual or potential economic value because of secrecy.**

### ***III. General Skill and Knowledge***

---

This section addresses the exclusion of non-secret information and the exclusion of general skill and knowledge. It is well-established in case law that trade secrets do not include information that is part of an employee's general skill and knowledge. Employees come to their jobs with varying degrees of skill, knowledge, and experience. Through work, training, and education, they enhance their skill, knowledge, and experience over time. Courts have long held that trade secrets cannot encompass what a court finds to be the general skill and knowledge of an employee.<sup>23</sup> This rule originated under the common law and has been carried forward into the modern statutory era. Yet there is virtually no statutory guidance other than occasional references—such as in the relatively new Texas trade secrets statute, which indicates that an injunction cannot “prohibit a person from using general knowledge, skill, and experience that person acquired during employment.”<sup>24</sup> In litigation, numerous cases drawing the distinction carefully assess the facts and circumstances of each case,<sup>25</sup> as well as the case law in the jurisdiction.<sup>26</sup>

---

<sup>23</sup> As noted above, the terminology varies, in some instances contracted to “general skill and knowledge,” and in others expanded to “general skill, knowledge, training, and experience.” Sedona will use the term “general skill and knowledge.”

<sup>24</sup> See Texas Civil Practice & Remedies Code § 134A.003 (added by Acts 2013, 83rd Leg., R.S., Ch. 10 (S.B. 953), Sec. 1, eff. September 1, 2013). The DTSA does include a limitation on injunctions that interfere with employment, but this is distinct from a rule that deprives an employee's general skills and knowledge of trade secret status at all. 18 U.S.C. § 1836(3)(A)(i) (2016). The legislative history to the DTSA's precursor, the Economic Espionage Act, expressly commented on the fact that general skills and knowledge are not trade secrets and offers insight into why this language does not appear as an “exclusion” in the statutory text. The legislative history states that

“[i]n the course of reconciling the Senate and House versions of this legislation, we eliminated the portion of the definition of trade secret that indicated that general knowledge, skills and experience were not included in the meaning of that term. Its elimination from the statutory language does not mean that general knowledge can be a trade secret. Rather, we believed that the definition of trade secrets in itself cannot include general knowledge. Thus, it was unnecessary and redundant to both define what does and what does not constitute a trade secret.”

See “General Knowledge Not Covered by Definition of Trade Secrets,” Managers' Statement for House Report 3723, Economic Espionage Act of 1996, 18 U.S.C.A. §§ 1831–1839, and Legislative History (1996).

<sup>25</sup> See, e.g., discussion in Restatement (Third) of Unfair Competition, § 42, cmt. d. (“Whether particular information is properly regarded as a trade secret of the former employer or as part of the general skill, knowledge, and experience of the former employee depends on the facts and circumstances of the particular case.”); see also discussion in the *Sedona Conference Journal Commentary on Equitable Remedies in Trade Secrets Litigation*, 23 SEDONA CONFERENCE JOURNAL, No. 2 (2021).

<sup>26</sup> A few examples of well-known cases that apply, or appear to apply, the rule that general skill and knowledge cannot be a trade secret include: *Wexler v. Greenberg*, 160 A.2d 430 (Pa. 1960); *Tempo Instrument, Inc. v. Logitek, Inc.*, 229 F. Supp. 1 (E.D.N.Y. 1964); *Winston Rsch. Corp. v. Minnesota Min. &*

In many situations, this rule overlaps with the basic statutory rule that information that is “generally known” in the industry cannot be a trade secret. For example, if a hair stylist claims trade secrets in basic hair-cutting techniques that she taught to an employee, this is not a trade secret because it is generally known to hair cutters across the industry.

However, in theory, information can be completely secret to the plaintiff employer, not known to others within the industry, but nonetheless qualify as general skill and knowledge the employee has gained through her employment and thus not be a trade secret. This principle has been referred to using different terminology. For example, the Restatement (Third) of Unfair Competition, drafted in 1995, proposes that “[i]f the information is so closely integrated with the employee’s overall employment experience that protection would deprive the employee of the ability to obtain employment commensurate with the employee’s general qualifications, it will not ordinarily be protected as a trade secret of the former employer.”<sup>27</sup> The Utah Supreme Court described this using different terminology but with a similar meaning. “Confidential information of an employer,” the Court wrote, “loses any protection to which it may have been entitled after it has been merged into the employee’s own faculties, skill and experience.”<sup>28</sup>

At the extremes, the distinction between trade secrets and general skill and knowledge tends to be noncontroversial. For example, Google’s search algorithm, first protected through patent law, has over time spawned many well-protected trade secrets that are not generally known to the relevant public or readily ascertainable using proper means. In contrast, how to cut hair is general skill and knowledge. Even special “tricks” that a particular salon may have developed for deciding when using a razor leads to better results than using scissors largely relates to the skill of the stylist wielding the tools rather than to a secret process.

However, the distinction becomes more difficult to answer when the information is not generally known in the industry—it is secret to one or a few firms—yet over-protecting it necessarily restricts someone’s ability to work in their field or profession. For example, in high-tech cases such as *Waymo v. Uber*, involving rapidly evolving, self-driving car technology, “first-mover” firms such as Waymo have developed information that may, so far as Waymo is aware, be unknown to other firms. When a Waymo employee such as Anthony Levandowski, who already had extensive knowledge of principles for developing operable autonomous vehicles, expands upon this pre-existing knowledge through his work at Waymo, and then moves to another firm in the same industry, he will not be expected to retreat to the college text-book version of designing autonomous vehicles. To the contrary, he will now know more advanced approaches than he did when joining Waymo. How much of this is Waymo’s trade secrets? How much of this might fairly be

---

Mfg. Co., 350 F.2d 134 (9th Cir. 1965); *Van Prods. Co. v. Gen. Welding & Fabricating Co.*, 213 A.2d 769, 776 (Pa. 1965); *Dynamics Research Corp. v. Analytic Scis. Corp.*, 400 N.E. 2d 1274 (Mass. App. Ct. 1980); *SI Handling Sys., Inc. v. Heisley*, 753 F.2d 1244 (3d Cir. 1985).

<sup>27</sup> Restatement (Third) of Unfair Competition, § 42, cmt. d. (Am. L. Inst. 1995). The group notes that the Third Restatement, like the other restatements discussed in the Commentary, is not “law” per se. That said, restatements can be a useful resource for understanding what the law is.

<sup>28</sup> *Microbiological Research Corp. v. Muna*, 625 P.2d 690, 697 (Utah 1981).

said to have become part of Levandowski’s unprotectable general skill and knowledge? When has it “been merged into [his] own faculties, skill and experience”? These are challenging issues.

The distinction brings two competing policy objectives into sharp conflict: First, employers have a right to protect and maximize the value of their trade secrets. Both of those rights often require, and typically benefit from, the disclosure of the company’s trade secrets to employees and others who can use or improve on them. Second, employees have a right to change jobs to advance their careers and generally should not be forced to leave a field altogether to find new employment. Exposure to trade secrets often enhances the employee’s general skill and knowledge and makes them a more valuable employee. To what extent should such newly developed skills and knowledge inhibit such an employee from using their enhanced skills and knowledge in pursuit of career advancement? The presence of an enforceable noncompete agreement has the potential to change the status quo. But when an explicit noncompete agreement is not present, the onus is on trade secret law, as opposed to contract law, to work out the right balance.

Distinguishing between general skill and knowledge and trade secrets is a challenging fact-intensive analysis, informed by many factors, including the relevant field/industry, the information at issue, how widely known outside the company the information is, the employee’s education, training, and experience, the employee’s contributions, the form the information takes,<sup>29</sup> and the employee’s conduct.<sup>30</sup>

**Key Issues for the Commentary to Address:** How can courts discern, at a practical level, whether specific information is properly classified as general skill and knowledge, as opposed to a trade secret? Can we derive principles and “rules of thumb” that will be useful to courts, employers, and employees? Can information be not generally known yet also become part of someone’s unprotected general skill and knowledge? Can information be protectable as to some employees and not others? Which party has the burden – does plaintiff have the burden to prove information is not general skill and knowledge, or is this an affirmative defense defendant must prove? How should courts take into account the policy concerns raised by general skill and knowledge at various phases of the case—for instance in the identification phase, in deciding the merits, and when crafting injunctions?

**[Proposed] Principle No. 3 – Determining whether information is properly classified as general skill and knowledge requires a careful balancing of facts and interests, and will necessarily be context specific.**

---

<sup>29</sup> Though perhaps somewhat oversimplified and overstated, the Restatement (Third) of Unfair Competition suggests that “[c]ourts are also more likely to conclude that particular information is a trade secret if the employee on termination of the employment appropriates some physical embodiment of the information such as written formulas, blueprints, plans, or lists of customers.” Restatement (Third) of Unfair Competition, § 42, cmt. d. (Am. Law. Inst. 1995).

<sup>30</sup> *Id.* (“[A]lthough information that is retained in the employee’s memory may be less likely to be regarded as a trade secret absent evidence of intentional memorization, the inference is not conclusive.”).

## ***IV. Confidential Information***

---

Many lawyers, business people and courts seem to contemplate that there is one category of information called “trade secrets,” which is protectable under trade secret law, and another category of information, perhaps overlapping but generally of lesser value, which is protectable only as “confidential information” based on different rules and different sources of law. Many organizations and employees speak in a lay sense of “crown jewels,” which they view as protected by trade secret law, and less valuable “confidential information,” which is not.

There are practical reasons for adopting this distinction. For example, an organization may choose to use the user-friendly term “confidential information” to describe valuable information internally to its non-lawyer employees or to non-technical employees like salespeople who might otherwise “tune out” discussions of how to protect “trade secrets,” because they may assume they don’t have any.

But the distinction between “trade secrets” and “confidential information” is more than a semantic issue. While the argument can be made that the definition of trade secrets under modern law is expansive enough to encompass a vast range of information, there are substantive reasons that an owner of information may want to rely on other legal regimes to protect the information, instead of or in addition to trade secret law. As discussed herein, some of these other remedies may be “preempted” (displaced) by trade secret law. But some are not. In particular, contracts, which are the product of private bargaining, and whose construction and enforceability are governed by state law, may help give information owners greater assurance of protection should the information be found to fall short of the criterion for trade secrecy.

State laws concerning protections for confidential information other than trade secret law vary tremendously. The Commentary will not attempt a comprehensive summary of the rules across jurisdictions or a state-by-state survey. But it will raise key issues and provide certain guidance.

### **A. HISTORICAL CONTEXT**

Under the common law, employees and other agents are recognized as having a duty to retain the confidentiality of certain information received during the course of a relationship. To give just one example, the Restatement (First) of Agency indicated that employees are under a “duty of confidence” with respect to “trade secrets, written lists of names, *or other similar confidential matters* given to [the agent] only for the principal’s use or acquired by the agent in violation of duty.”<sup>31</sup>

---

<sup>31</sup> Restatement (First) of Agency § 396 (Am. Law Inst. 1933) (emphasis added). The Restatement (Second) of Agency, drafted in 1958, provided more details. It indicated that this duty applied to information “confidentially given” to the agent by the principal—though notably it provided that the duty did *not* apply



The Restatement (First) of Torts—which was drafted in 1939 and reflected more or less the state of the common law regarding trade secrets prior to passage of the UTSA—expressly distinguished between trade secrets and “other secret information in a business.”<sup>32</sup> The First Restatement defined a trade secret narrowly, requiring both use in a business and opportunity for competitive advantage over others.<sup>33</sup> This meant, for example, that prototypes and pre-commercial information, could not be a trade secret. Nor could “ephemeral” information with only short-term value.<sup>34</sup> But the First Restatement had also delineated a separate category of protectable “confidential” information that does *not* necessarily qualify as a trade secret, so long as it was “relat[ed] to matters in [the holder’s] business” and was “*of a secret or confidential character*.”<sup>35</sup>

The UTSA, which was drafted in 1979 (and amended in 1985), narrowed and some say eliminated the distinction between trade secrets and otherwise “confidential” information. Among other things, the UTSA eliminated the requirement that the trade secret be “continuously used in one’s business,” to protect information that was not yet in use or fully commercialized, or that had only short-term value—for instance, plans for an impending bid proposal that could have significant value to the bidder and to a competing bidder, even if they lacked enduring, long-term value. The comments to the UTSA also reflected an intention to protect “information that has commercial value from a negative viewpoint, for example the results of lengthy and expensive research which proves that a certain process will not work could be of great value to a competitor.”<sup>36</sup>

In light of the expanded definition of a trade secret, the UTSA did not delineate and arguably had no need to discuss a category of information that was “of a secret or confidential character” if not technically a trade secret. Some business people, employees, and courts continue to speak or think in terms of “mere” confidential information that “does not rise to the level” of a trade secret, suggesting that trade secret law may be

---

to “a matter of general knowledge.” Restatement (Second) of Agency § 395 (Am. Law Inst. 1958). See also Restatement (Third) Of Agency § 8.05 (Am. Law inst. 2006).

<sup>32</sup> A Comment to Section 757 states: “[A trade secret] differs from other secret information in a business (see § 759) in that it is not simply information as to single or ephemeral events in the conduct of the business, as, for example, the amount or other terms of a secret bid for a contract or the salary of certain employees, or the security investments made or contemplated, or the date fixed for the announcement of a new policy or for bringing out a new model or the like.” Restatement (First) of Torts, § 757, cmt. b (Am. Law. Inst. 1939).

<sup>33</sup> Section 757 states that a trade secret was “any formula, pattern, device or compilation of information which is used in one’s business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it.” Restatement (First) of Torts § 757 (Am. Law Inst. 1939).

<sup>34</sup> See Restatement (First) of Torts, § 757, cmt. b (Am. Law. Inst. 1939), quoted in note *supra*.

<sup>35</sup> Section 759 provided a separate cause of action for “harm” caused by another’s “possession, disclosure or use” of “information about another’s business.” This class of information was broadly defined. “There are no limitations as to the type of information included ....” But the information did have to “relate to matters in [the holder’s] business” and be “of a secret or confidential character” to qualify. Restatement (First) of Torts § 759 (Am. Law Inst. 1939).

<sup>36</sup> UTSA § 1, cmt. See also Restatement (Third) of Unfair Competition § 39, cmt. e (Am. Law Inst. 1995) (discussing this historical trajectory and expansion of the definition of a trade secret).

inadequate to protect this information and perhaps misleadingly implying that this type of information is not as important as true trade secrets.<sup>37</sup>

But the reality is that companies possess a significant amount of confidential information, which may or may not meet the technical definition of a trade secret, and companies will seek to protect this in whatever ways make sense. An example may be knowing that a particular vendor's quality control is consistently superior to that of another vendor; or knowing that the company plans to develop certain production capabilities itself rather than relying on vendors. Another example may be a dataset that is highly costly and time-consuming to develop, but that might be deemed "readily ascertainable using proper means" according to the doctrines discussed above.

This "confidential information" is surely useful, in many cases quite valuable. The organization will likely want to exercise control over who knows it and whether they can reveal it to others. While a case might be made that such information *does* meet the legal definition of a trade secret, this conclusion may not be free from doubt. Risk-averse organizations might rationally seek assurance that this information can remain secret and legally protected by adopting certain measures, including contracts, and by invoking various non-trade secret legal theories instead of or, more likely, in addition to trade secret law. A key question then becomes whether these other legal regimes will in fact serve this function and under what conditions.

**Key Issues for the Commentary to Address:** Is it appropriate to think of a separate category of non-trade secret yet "confidential" information? What, in specific, are the types of confidential information that firms might realistically wish to protect and how/when might trade secret law be inadequate to protect it? What alternatives to trade secret law may help? Does the law impose limitations on information that an organization may claim as "confidential" if that information does not qualify as a trade secret? What is the role of other regulations such as privacy laws (e.g., The Health Insurance Portability and Accountability Act of 1996, HIPAA) in dictating what information firms can keep legally "confidential" even if it is not a trade secret? Is there ever a legitimate justification for protecting non-trade secret information that is or has become public or generally known?

**[Proposed] Principle No. 4 – Employees and others may have a duty of confidentiality with respect to confidential information under legal regimes other than trade secrets law. Other causes of action, in particular contract law, may exist to enforce that duty or protect such confidential information in certain circumstances.**

---

<sup>37</sup> Some courts use the phrase "not rising to the level of a trade secret," especially in discussions of preemption, though this can be misleading. For an example and a discussion of this history, see, e.g., *Mortg. Specialists, Inc. v. Davey*, 153 N.H. 764, 776, 904 A.2d 652, 663 (2006) (noting the view that "[w]ith the enactment of the UTSA, confidential information not rising to the level of a statutory trade secret was left largely unprotected by the law.").

## **B. PREEMPTION OF OTHER REMEDIES RELATED TO TRADE SECRETS AND CONFIDENTIAL INFORMATION**

A logical first question when considering whether confidential information can be protectable under some alternative legal regime, such as contract law or potentially tort or unfair competition law, is whether these alternative regimes are “preempted” or displaced by trade secret law or another field of law.<sup>38</sup>

The law of preemption in this area is extremely murky and is applied differently under the laws of various states. This is not a Commentary on preemption, in specific. But in considering whether legal regimes other than or in addition to trade secret law may be available to protect particular information, any limitations trade secret law may impose on alternative remedies must be considered. The Commentary will not purport to supply a comprehensive coverage or a state-by-state survey of different state rules. But it will raise some key considerations and seek to provide useful guidance.

The DTSA declines to preempt state trade secret law or other state law causes of action.<sup>39</sup> However, the UTSA, as amended in 1985, contains a provision stating that a trade secret law adopting this provision preempts certain remedies and permits others. UTSA, Section 7 states that

(a) Except as provided in subsection (b), this [Act] displaces conflicting tort, restitutionary, and other law of this State providing civil remedies for misappropriation of a trade secret.

(b) This [Act] does not affect:

(1) contractual remedies, whether or not based upon misappropriation of a trade secret; or

(2) other civil remedies that are not based upon misappropriation of a trade secret; or

(3) criminal remedies, whether or not based upon misappropriation of a trade

---

<sup>38</sup> Other possible bases for preemption include federal patent law and federal copyright law. Patent preemption typically affect contracts and other relational rights that do not prohibit copying of a public-domain article. *See Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 484 (1974); *see also* *Aronson v. Quick Point Pencil Co.*, 440 U.S. 257, 257, 264 (1979) (indicating that federal patent law does not generally preempt state contract law so as to preclude enforcement of a contract requiring payment of royalties for unpatented invention). Copyright law’s preemption provision, 17 U.S.C. § 301 (1976), does not preempt state law claims “if an ‘extra element’ is ‘required instead of or in addition to the acts of reproduction, performance, distribution or display, in order to constitute a state-created cause of action, then the right does not lie ‘within the general scope of copyright,’ and there is no preemption.” *Computer Assocs. Int’l, Inc. v. Altai, Inc.*, 982 F.2d 693, 716-717 (2d Cir. 1992).

<sup>39</sup> *See* 18 U.S.C. § 1838 (2016). The exception is the whistleblower provision, which expressly preempts state and federal civil and criminal law with respect to disclosures by employees or independent contractors made in confidence to governments or in court or to a lawyer in connection with retaliation lawsuits. *See* 18 U.S.C. § 1833 (2016).

secret.<sup>40</sup>

The states diverge in whether and how they incorporate Section 7. Even in states that incorporate a version of Section 7, there is significant disagreement regarding what is or is not preempted. The main distinction is between contractual remedies, and other civil remedies.

With regard to non-contract remedies—such as tort law, fiduciary duty law, or unfair competition law—there is significant divergence among the states, independent of the related, complicating issue that states have adopted different versions of the UTSA. One view is that remedies associated with claims that resemble trade secret claims are *not* preempted when the information at issue is not a trade secret.<sup>41</sup> Another view is that non-contract remedies associated with claims that resemble trade secret claims are largely preempted (at least in jurisdictions that have adopted a similar version of UTSA Section 7), but that remedies for wrongful conduct independent of the misappropriation of trade secrets may survive.<sup>42</sup> Thus, even in jurisdictions that tend towards preemption, if there has been wrongdoing *unrelated to using or disclosing confidential information*, remedies based on that other wrongdoing may not necessarily be preempted.<sup>43</sup>

With regard to contracts, in contrast, the majority view is that contractual remedies survive, regardless of whether that information at issue qualifies as a trade secret. This is due to the fact that the UTSA's preemption provision—which in this respect is universally

---

<sup>40</sup> UTSA, § 7 (as amended in 1985).

<sup>41</sup> See, e.g., *Burbank Grease Servs., LLC v. Sokolowski*, 2006 WI 103, ¶ 33, 294 Wis. 2d 274, 298, 717 N.W.2d 781, 793 (Wis. 2006) (construing Wisconsin UTSA) (“[T]he plain language of Wis. Stat. § 134.90(6)(a) and (b) 2, taken together, are meant to do the following: (1) replace all pre-existing definitions of “trade secret” and remedies for tort claims dependent solely on the existence of a specific class of information statutorily defined as “trade secrets”; and (2) leave available all other types of civil actions that do not depend on information that meets the statutory definition of a “trade secret.”); *Cenveo Corp. v. Slater*, No. 06-CV-2632, 2007 U.S. Dist. LEXIS 9966, at \*13, 2007 WL 527720, at \*3 (E.D. Pa. Feb. 12, 2007) (E.D. Pa. Feb. 12, 2007) (construing Pennsylvania UTSA) (“The Court finds that the cases holding that the Trade Secrets Act does not preempt common law tort claims when it has yet to be determined whether the information at issue constitutes a trade secret take the better approach. Preempting plaintiff’s conversion claim at the motion to dismiss stage risks leaving the claimant without a remedy for information he proves has been stolen.”).

<sup>42</sup> See, e.g., *BlueEarth Biofuels, LLC v. Hawaiian Elec. Co.*, 123 Haw. 314, 328–29, 235 P.3d 310, 324–25 (2010) (construing Hawaii UTSA) (“Tort, restitutionary, and other law[s] of this state” conflict with the HUTSA, are therefore displaced, to the extent that they are based upon misappropriation of a trade secret. ... For those claims found to conflict with the HUTSA, the scope of displacement is complete. However, a claim may survive to the extent it alleges wrongful conduct independent of the misappropriation of trade secrets. ... The HUTSA displaces non-contract civil claims based upon the alleged acquisition, disclosure, or use of confidential information that does not rise to the level of a statutorily-defined trade secret”).

<sup>43</sup> See, e.g., *Hecny Transp., Inc. v. Chu*, 430 F.3d 402, 404–405 (7<sup>th</sup> Cir. 2005) (construing Illinois UTSA) (“The [provision] does not apply to duties imposed by law that are not dependent upon the existence of competitively significant secret information, like an agent’s duty of loyalty to his or her principal.” We would be shocked if the Supreme Court of Illinois were to disagree; nothing in its jurisprudence suggests that it would. This is not a close question. An assertion of trade secret in a customer list does not wipe out claims of theft, fraud, and breach of the duty of loyalty that would be sound even if the customer list were a public record.”) (internal citations omitted).

adopted—excludes “contractual remedies” from the purview of preemption, whether or not based on a trade secret. The 1985 Commentary to the UTSA appears to make this non-preemptive stance even clearer, stating, in relevant part, that the UTSA “applies to a duty to protect competitively significant secret information that is imposed by law. *It does not apply to a duty voluntarily assumed through an express or an implied-in-fact contract.*”<sup>44</sup> Relatedly, tortious interference with contract claims may also survive preemption in some situations.<sup>45</sup> The rules are jurisdictionally specific, as well as fact specific. Even courts in the same state, applying the same laws, may reach divergent outcomes on similar facts.<sup>46</sup> Nonetheless as discussed below, contract claims may be unenforceable for other reasons—not least because they run afoul of a jurisdiction’s rules regarding restraints against trade.

In sum, whether a legal claim related to confidential information is preempted by state trade secret law is dependent upon many variables—the most important of which may well be the law being applied and the court deciding the case.

**Key Issues for the Commentary to Address:** What are the various approaches to preemption adopted by different jurisdictions, and can we articulate unifying or common principles? What other types of wrongdoing (such as physical takings of documents or breach of fiduciary duty) may be actionable irrespective of preemption by trade secret law? What is the significance of physical takings in protecting information, and are there different legal consequences and remedies? What is the implication, if any, of the fact that

---

<sup>44</sup> UTSA, § 7, cmt. (amended 1985) (emphasis added) (“The enforceability of covenants not to disclose trade secrets and covenants not to compete that are intended to protect trade secrets, for example, is governed by other law. The Act also does not apply to a duty imposed by law that are is not dependent upon the existence of competitively significant secret information, like an agent's duty of loyalty to his or her principal.”).

<sup>45</sup> See, e.g., *Revere Transducers, Inc. v. Deere & Co.*, 595 N.W.2d 751, 765 (Iowa 1999) (Iowa trade secret law did not preempt tortious interference with contract claim); *IDX Sys. Corp. v. Epic Sys. Corp.*, 285 F.3d 581 (7th Cir. 2002) (Wisconsin trade secret law did not preempt plaintiff's claim that a competitor tortiously induced a customer to breach an otherwise enforceable confidentiality agreement); *Cardiac Pacemakers, Inc. v. Aspen II Holding Co.*, 413 F. Supp. 2d 1016, 1023-1026 (D. Minn. 2006) (under Minnesota law claim for tortious interference with confidentiality agreement was not preempted by trade secret law).

<sup>46</sup> Courts in California, for example, may find that a tortious interference with contract claim brought against a third party is preempted by California trade secret law to the extent it rests on the same facts as a trade secret claim, but not when other wrongdoing or other information is involved. Compare, e.g., *K.C. Multimedia, Inc. v. Bank of Am. Tech. & Operations, Inc.*, 171 Cal. App. 4th 939, 960, 90 Cal. Rptr. 3d 247, 263 (2009) (holding claim for tortious interference with contract claim was preempted because it rested “on the same legal and factual basis as [plaintiff's] trade secret misappropriation claim”) with, e.g., *Javo Beverage Co. v. California Extraction Ventures, Inc.*, No. 19-CV-1859-CAB-WVG, 2019 WL 6467802, at \*4–5 (S.D. Cal. Dec. 2, 2019) (denying motion to dismiss plaintiff's contractual interference with contract claim because it involved allegations beyond trade secret misappropriation and was “based upon non-trade secret information.”).

the UTSA's preemption provision applies to "remedies" rather than "claims"? How does preemption affect tortious interference with contract claims?

**[Proposed] Principle No. 5 – Whether a legal claim related to confidential information is preempted by state trade secret law depends on many factors, including which version of the UTSA's preemption provision the state has adopted and court decisions interpreting that provision, the nature of the information at issue, the legal regime on which the claim is based, especially whether it is a contract or a non-contract claim, the source of the duty on which the claim is based, and the conduct and factual circumstances giving rise to the claim, in particular whether there is wrongdoing that is separate from use or disclosure of confidential information.<sup>47</sup>**

### **C. ENFORCEABILITY OF CONTRACTS COVERING CONFIDENTIAL INFORMATION**

Contracts can be and are frequently used to protect confidential information. They take many forms—ranging from non-compete agreements and non-solicitation agreements to “plain vanilla” nondisclosure and confidentiality provisions. Ordinarily private parties are given considerable latitude to negotiate and agree to contracts. However, in some instances the law imposes limitations on parties' ability to enforce contracts to protect information.

Noncompete agreements are heavily scrutinized in every jurisdiction because they are treated as restraints on trade. States differ widely in the extent of restraints they will permit. Because laws governing noncompete agreements are currently state-specific, are rapidly evolving, and are well documented in other commentaries, we do not probe differences among such laws here. That said, at a high level, case law in the arena of noncompetes counsels that freedom of contract is not unlimited. As one court memorably put it— declining to issue an injunction to enforce a noncompete agreement against a dancing instructor who did not appear to have received any discernable secrets—an employer cannot, through “self-serving ‘Whereas’ clauses...state that he is going to confide something unique and hush-hush, and then merely disclose the A. B. Cs or Mother Goose Rhymes, and make that the basis of irreparable injury.”<sup>48</sup>

Other contracts, including nondisclosure and confidentiality agreements may also be subject to public policies limiting their potential reach. There are circumstances under which claims for breach of contract, even if they are not fully preempted under the rules mentioned above, may be limited by other legal regimes—such as laws against unlawful restraints on trade or against unfair competition—when they protect more than trade secrets or when they reach too broadly.

---

<sup>47</sup> The group understands that this is not a “principle” yet, but rather a list of considerations. This will evolve as the Commentary moves forward.

<sup>48</sup> Arthur Murray Dance Studios of Cleveland v. Witter, 105 N.E.2d 685, 710 (Ohio Com. Pl. 1952).

For example, an opinion from the Sixth Circuit, applying Texas law, has held that “confidential information” can be defined by contract even if it does not “achiev[e] trade-secret status,” but only “so long as it does not encompass publicly available information or an employee’s general knowledge or skills[.]” The opinion further suggests that “the rules governing trade secrets are still relevant in analyzing the reasonableness and enforceability of non-disclosure provisions because, in order to justify the contractual restraint, information subject to non-disclosure provisions must share at least some characteristics with information protected by trade secret statutes.” A so-called non-disclosure agreement prohibiting “employees from using general knowledge, skill, and experience acquired in their former employment,” the court writes, “is more properly characterized as a non-compete agreement[.]” and should be restricted accordingly.<sup>49</sup>

Some cases have noted that broadly worded nondisclosure agreements bringing within their sweep information going beyond trade secrets might be treated as a restraint against trade or even a de facto noncompete agreement. For example, in California, courts have found that confidentiality agreements that prevent use or disclosure of broadly defined “confidential information” may be invalidated as “de facto noncompete” agreements that run afoul of California’s ban on noncompetes.<sup>50</sup>

Even in states that do not ban noncompete agreements, courts may interpret contracts that prevent use or disclosure of “confidential information” to be a restraint against trade and may apply their jurisdiction’s standard for “reasonableness,” perhaps even requiring that the restraint be limited in time or (less likely) geographic scope. For example, a line of Wisconsin cases has applied the state’s statutory restriction on “restrictive covenants” to nondisclosure agreements that prevent use of information that is general knowledge in the industry.<sup>51</sup>

Similar results have been reached in states that have common law rules for assessing the “reasonableness” and enforceability of noncompetes. For example, in an Illinois case, a state appeals court upheld the determination that a nondisclosure agreement was an unenforceable restraint of trade and void as a matter of law, when the agreement sought to prevent, during and after employment, the use or disclosure of a broad list of information.<sup>52</sup> In a more recent South Carolina case, a court held that a nondisclosure

---

<sup>49</sup> See *Orthofix, Inc. v. Hunter*, 630 F. App’x 566, 567–68 (6th Cir. 2015).

<sup>50</sup> See, e.g., *Brown v. TGS Management Company, LLC*, 57 Cal. App. 5th 303, 317 (2020) (“the confidentiality provisions in the Employment Agreement on their face patently violate section 16600. Collectively, these overly restrictive provisions operate as a de facto noncompete provision; they plainly bar Brown in perpetuity from doing any work in the securities field, much less in his chosen profession of statistical arbitrage. Consequently, we conclude the confidentiality provisions are void *ab initio* and unenforceable.”).

<sup>51</sup> See, e.g., *Nalco Chem. Co. v. Hydro Techs., Inc.*, 984 F.2d 801, 801–04 (7th Cir. 1993), as amended on denial of reh’g (Mar. 18, 1993) (applying Wis. Stat. § 103.465); *Staffworks Group-Wisconsin Inc. v. Serv. First Staffing*, 2020 U.S. Dist. LEXIS 113666, \*1 (E.D. Wis. 2020) (applying Wis. Stat. § 103.465).

<sup>52</sup> See *North American Paper Co. v. Unterberger*, 172 Ill. App. 3d 410, 415–16, 526 N.E.2d 621, 624–25 (1988) (“[T]he nondisclosure aspect of the Agreement has no chronological or geographical limitations of any kind, it purports to protect virtually every kind of information that Unterberger learned during the period of his employment even if non-confidential, and it goes far beyond any possible legitimate protectible

agreement was unenforceable because it was in effect a noncompete agreement and ran afoul of South Carolina's standards for enforcing noncompetes.<sup>53</sup> In a very recent case, the First Circuit, applying Puerto Rico law, discussed in some detail the circumstances in which a nondisclosure may be overly broad and unenforceable, writing, in relevant part, that

[a] nondisclosure agreement is overly broad if the restriction is “[un]necessary for the protection of the employer's business,” “unreasonably restrictive of the employee's rights,” and “prejudicial to the public interest.” Numerous courts have identified the types of agreements in which restrictive clauses are overly broad. First, an employer's interest does not extend to prohibiting the employee from using general knowledge acquired by the employee[.]... Second, a nondisclosure agreement is overly broad and invalid when the agreement prohibits disclosure of information that “is not in fact confidential,” because it is public knowledge. Third, a nondisclosure agreement is overly broad when it extends to information properly provided to the defendant by third-party sources. ...All of these factors exist here.”<sup>54</sup>

**Key Issues for the Commentary to Address:** To what degree can contracts be used to protect information that is not necessarily a trade secret, but that is reasonably confidential? When are contracts covering confidential information likely to be viewed as restraints on trade akin to noncompetes? What types of nondisclosure provisions raise questions with regard to enforceability? In what circumstance may they be found unenforceable? Does failing to include certain “carveouts” from nondisclosure agreements—such as for information that is generally known or that has become public through no fault of the recipient—jeopardize enforceability of the contract? Will the contract necessarily be enforceable if it *does* include such carveouts? When confidentiality

---

interest of NAPCO. Thus, we agree with the trial court's sound conclusion that the nondisclosure aspect of the Agreement constitutes an impermissible restraint of trade and is void as a matter of law.”). Notably, this agreement did on its face carve out “information within the public domain and generally known within the paper and packaging industry.” But the court found it “undisputed that NAPCO had virtually no confidential methods or systems relating to chemical products when the Agreement was signed,” and there was “no evidence that Unterberger has ever used or divulged any confidential information obtained from NAPCO.” *Id.* at 415.

<sup>53</sup> Even though the contract in this case actually did allow the employee to use “the general skills and knowledge” he acquired while working for the plaintiff, it provided that if the employee “engaged in an employment relationship” with a “Competing Business” “in a position similar” to his position with plaintiff, that would “necessarily and inevitably result in [him] revealing, basing judgments and decisions upon, or otherwise using [plaintiff's] Confidential Information to unfairly compete with [plaintiff].” Therefore, the court interpreted this as in effect a noncompete, and one that was invalid under South Carolina law because it was unlimited in time. *See* *Fay v. Total Quality Logistics, LLC*, 419 S.C. 622, 631, 799 S.E.2d 318, 323 (Ct. App. 2017).

<sup>54</sup> *TLS Mgmt. & Mktg. Servs., LLC v. Rodriguez-Toledo*, 966 F.3d 46, 58–59 (1st Cir. 2020) (internal quotations removed) (citing numerous cases, including, *e.g.*, *Revere Transducers, Inc. v. Deere & Co.*, 595 N.W.2d 751, 762 (Iowa 1999); *Nagler v. Garcia*, 370 F. App'x 678, 681 (6th Cir. 2010); *AssuredPartners, Inc. v. Schmitt*, 398 Ill.Dec. 434, 44 N.E.3d 463, 475–76 (Ill. Ct. App. 2015)).



agreements incorporate language from the DTSA or UTSA, does this impose limitations from trade secret law on the contract? Are courts less likely to evaluate the “fairness” of nondisclosure agreements between organizations, as opposed to between employer and employee? Can confidential information be described more broadly in agreements between organizations than in agreements between an employer and employees? Is contractual protection more justified for non-trade-secret information that was costly to develop (e.g., datasets that involve significant "sweat labor" but that may arguably fail to satisfy one of the statutory requirements of a trade secret)? In light of those rules, how should agreements covering confidential information be drafted? What remedies are available for breach of agreements protecting confidential information? Can “trade secret remedies” (such as unjust enrichment damages) be productively negotiated into nondisclosure agreements? What are the consequences of doing so?