IP Protection

By Henry M. Sneath and Robert L. Wagner

The New Federal Defend Trade Secrets Act of 2016

Corporate Counsel Roundtable

Companies have a variety of tools at their disposal to protect their intangible intellectual property rights under both state and federal laws. Traditionally, federal law either exclusively or primarily governed the patent, trademark, and copyright laws, while state laws almost exclusively protected trade secrets. With the signing of the federal Defend Trade Secrets Act of 2016 (DTSA) on May 11, 2016, by the President, companies now have another tool in their arsenal to protect their trade secrets in federal courtrooms across the country.

What Are Trade Secrets?

In additional to its tangible assets, most companies have significant intangible assets developed over years that improve their ability to compete in the marketplace. While not an exclusive list, the big four intellectual property rights (patents, trade secrets, trademarks, and copyrights) are the primary rights that protect a company's core intangible assets.

Trademarks are perhaps the most common intellectual property right possessed by a company. They serve as source identifiers for goods and services sold by a company, and the trademark laws protect a company's branding by providing a means for preventing others from using the same or similarly confusing marks in commerce—thereby either diluting the goodwill created by the company or passing off their goods as being the company's.

Copyrights protect original, creative expressions, such as literary, musical, graphical, audiovisual, and dramatic works, but not the factual or substantive content within the expression. Depending on the nature of the goods or services provided by a company, copyrights can be extremely important or of lesser importance. For example, in creative and media companies that focus on written, musical, or video content, copyrights form the primary means of protecting their goods and services.

Patents provide a means for controlling the use and sale of new and novel inventions—such as products, processes, machines, and compositions—for a limited time (roughly a 20-year period). In order to obtain a patent, an inventor must demonstrate to the Patent Office that the invention is new and not obvious through a thorough examination process. One drawback of this process is that the inventor must publicly disclose the details of the invention and the best way of making or using the invention during the application process, so regardless of whether a patent ever issues, the public will learn about the invention and how to use it. On the other hand, a significant benefit of the patent system is that patent infringement is a strict

■ Henry M. Sneath is a business trial attorney with Picadio Sneath Miller & Norton, P.C. in Pittsburgh, focusing on business, intellectual property, insurance, energy sector, products liability, and tort litigation matters. He is a past president of DRI. Robert L. Wagner is counsel at Picadio Sneath Miller & Norton, P.C. He focuses his practice on patent, intellectual property, and commercial litigation matters. He is currently the chair of the DRI Intellectual Property Litigation Committee's Patents Specialized Litigation Group.

liability offense—the patent owner can prevent anyone from using the invention, regardless of whether the other person or company independently invented the same invention or was even aware of the patent.

Finally, trade secrets are in some ways similar to patents, but are both broader and narrower in scope in different ways. A trade secret is a valuable piece of information (such as a formula, drawing, method, technique, or process) that is not well-known by the public or in the industry, that is valuable to a company by virtue of its secrecy, and that the company takes reasonable measures to keep secret. Trade secrets can provide broader protection than patents, because they are not limited to new and novel inventions or things, and they can potentially last forever. In addition, there is no application or registration process for trade secrets, so there is no public disclosure (and, indeed, they cannot be public disclosed and still be a trade secret). But, trade secrets provide narrower protection to a company, because the law only protects against the misappropriation of a trade secret. Therefore, a third party's independent development or reverse engineering is not considered to be misappropriation and is not unlawful in the absence of some contractual agreement not to do so.

Brief History of Trade Secret Protection

Traditionally, trade secrets were primarily protected under state law. Recognizing the need for some uniformity in how trade secrets should be protected across the country, the Uniform Law Commission published the Uniform Trade Secrets Act (UTSA) in 1979, which provided a uniform framework for states to adopt. The UTSA was later amended in 1985, and it has now been adopted by 47 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands. Only Massachusetts, New York, and North Carolina have yet to adopt the UTSA, although each of those states has its own trade secret law.

While each of the 47 states mentioned above adopted a form of the UTSA, they did not all exactly adopt the UTSA. Many states chose not to adopt certain portions of the UTSA or chose to modify sections of it. As a result, while the overall framework is similar in these 47 states, there are differences—sometime subtle, sometimes substantial—between the laws. In addition, some states have had more active litigation, and, therefore, a more developed case law interpreting various provisions in their trade secret laws than others. For instance, what information qualifies as a trade secret, the steps that are necessary in "reasonably" protecting the trade secret, and the limitations that can be placed on former employees when they leave a company all can vary from state to state.

> With the signing of the federal Defend Trade Secrets Act of 2016 (DTSA) on May 11, 2016, by the President, companies now have another tool in their arsenal to protect their trade secrets in federal courtrooms across the country.

In light of the state-to-state variations and uncertainty in the law, Congress perceived a need to create a more uniform trade secret law that would supplement these states' laws and provide more consistent and predictable rules. Congress chose not to start from scratch, but instead modeled its efforts on the UTSA. The DTSA was born from these efforts, almost unanimously passing both houses of Congress and becoming law on May 11, 2016. The DTSA primarily amends the Economic Espionage Act of 1996 (18 U.S.C. §1830 *et al.*), although it has some effect on other statutes.

Because trade secrets were governed by state law, most lawsuits involving the misappropriation of trade secrets had to be filed in state court unless a separate basis for federal jurisdiction existed—such as by bringing another claim based on federal law or where the parties were diverse. With the DTSA, litigants will now be able to bring claims directly in federal court, which is a great advantage. Federal courts in general have greater resources and familiarity to deal with these kinds of cases, which can often involve complex and sensitive technologies and information. In addition, with the national scope of the law and the more consistent practice of federal courts to report and explain their decisions, a more uniform and well developed body of law should quickly emerge that will provide more guidance and predictability for the application of the DTSA nationwide.

While Congress determined that a national trade secret law would be beneficial, it chose not to preempt state laws that protect trade secrets, which allows litigants to raise both federal and state trade secret misappropriation claims in a single lawsuit. As will be discussed below, the DTSA is in many ways very similar to its state-law counterparts, but there are some differences that will likely make it advantageous for a plaintiff to bring claims under both the DTSA and the relevant state's trade secret law.

The Standards and Requirements Under the DTSA

As is true with most statutory frameworks, the DTSA sets forth and defines much of what constitutes a violation of the DTSA within the statute itself. The DTSA provides that the owner of a trade secret related to a product or service that is used in interstate or foreign commerce may bring a civil action for misappropriation of that trade secret.

There are four key elements to any civil claim brought under the DTSA: (1) the information must be a trade secret; (2) the owner of the trade secret must bring the claim; (3) the trade secret must involve goods or services used in interstate or foreign commerce; and (4) the information must have been misappropriated.

In general, a trade secret is any kind of information that provides a competitive advantage to a company and that has been kept secret. The DTSA broadly defines a trade secret to include "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, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing" that the owner takes reasonable measures to keep secret and derives independent economic value from not being generally well known or ascertainable. This definition is different than that found in the UTSA, which has a simpler definition, although, as a practical matter, it is not clear that there will be a meaningful difference between the two.

One of the chief stumbling blocks that companies (especially smaller ones) run into is showing that they have taken reasonable steps to keep their information secret. Companies need to look carefully at defining exactly what their trade secrets are and then make sure that only the people who have a need to know the information are given access to it. The crown jewels of the company should not be on servers or in file cabinets that anyone in the company can access. In addition, companies should have clear policies and procedures in place (such as in non-disclosure and non-compete agreements and in employee handbooks) that set forth that certain kinds of information are confidential and proprietary and cannot be shared or used except for the benefit of the company.

Only an owner of the trade secret can bring a claim for trade secret misappropriation, which can become an issue when a company has multiple subsidiaries or related companies. In these instances, plaintiffs will need to determine carefully which company owns the trade secret and, therefore, has standing to sue. In addition, in order for Congress to have the power to enact the DTSA, it had to tie violations of the law to interstate or foreign commerce. Therefore, to bring a claim under the DTSA, the trade secret owner must show that the trade secret was used in interstate or foreign commerce. For most goods and services in the global marketplace, that will not be an issue. But, it could become a problem when the trade secret only involves purely intrastate services or the product is still in development and has not yet been sold.

Finally, the DTSA only protects against misappropriations, which are defined in the statute as either the acquisition of a trade secret either directly or indirectly through improper means, or the disclosure or use of a trade secret acquired through improper means. Unlike the UTSA, the DTSA specifically defines what is and is not "improper means." Improper means include means such as theft, bribery, misrepresentation, breach of a duty of secrecy, and espionage, but do not include reverse engineering or independent development. As a practical matter, states adopting the UTSA have similarly found reverse engineering and independent development not to be improper means, but the DTSA explicitly clarifies this in its statutory language.

The court can impose limitations and conditions on employment, but they have to be based on actual evidence of threatened misappropriation and not based merely on the information that the person happens to know.

Under the DTSA, there are a variety of possible remedies available to a prevailing plaintiff, including injunctive relief, compensatory damages, unjust enrichment damages, reasonable royalties, exemplary damages (up to twice the compensatory damages), and attorneys' fees in cases of willful and malicious misappropriation. With respect to injunctive relief, a court can enter an order preventing the actual or threatened misappropriation consistent with state law, but cannot prevent a person from being employed with another company because he or she is aware of another's trade secret. The court can impose limitations and conditions on employment, but they have to be based on actual evidence of threatened misappropriation and not based merely on the information that the person happens to know. In addition, they cannot conflict with the relevant state's law relating to restraints on an individual's right to practice his or her profession, trade, or business. Depending on the state in which the employee resides and works, these limitations can pose significant hurdles for a plaintiff to overcome if it wants to obtain injunctive relief against a former employee.

In addition, the DTSA has extra-territorial application that greatly expands the scope of its protections. By being part of the Economic Espionage Act of 1996, the DTSA includes the provisions that extend liability to conduct occurring outside of the United States (18 U.S.C. §1837). If the accused offender is a citizen or permanent resident of the United States, or an organization organized under state or federal law, or some act in furtherance of the misappropriation occurred in the United States, the DTSA applies and a lawsuit may be brought in the United States against the offender. Therefore, if a U.S. citizen misappropriates a company's trade secret while outside of the United States or if a foreign company steals a trade secret and at least one act in furtherance of that theft occurred in the United States, a company can bring suit against the citizen or foreign company in the United States under the DTSA. By no means will this extra-territorial scope prevent foreign entities from stealing a U.S. company's trade secrets, but it will create another tool for companies to use in both discouraging such conduct and obtaining some remedy if it occurs.

Finally, the DTSA has a three-year statute of limitations, like the UTSA, so it does not provide a longer or shorter period of time to bring a claim. It treats a continuing misappropriation as one act, rather than a series of acts, which can become relevant for purposes of the statute of limitations. Not all states have taken a similar position, so this could be one area where a federal claim might be barred under the statute of limitations, but a state claim would not be.

Ex Parte Seizure Orders

One of the more controversial and distinct aspects of the DTSA is the ability for a trade secret owner to obtain an *ex parte* seizure order from a court to prevent the dissemination and propagation of a misappropriated trade secret prior to any determination of the merits of the case or even notice to the defendant. Law enforcement personnel will implement this order, and not the trade secret owner. Therefore, the order must specifically describe the objects to be seized and their location with sufficient particularity and narrowness to enable law enforcement personnel to identify and seize only the relevant items. As might be expected, obtaining such an order is not easy, and there are significant hurdles that a trade secret owner must overcome become it can obtain one.

First, the trade secret owner must demonstrate that it will suffer immediate and irreparable harm if the court does not order the seizure and that other forms of equitable relief (such as a temporary restraining order or preliminary injunction) would not be adequate because the offending party would "evade, avoid, or otherwise not comply with such an order."

Second, the trade secret owner must show that the harm to it if the court does not grant the order substantially outweighs the harm to the other side's legitimate interests if the order is granted. Depending on the nature of the trade secret, this factor may be difficult for a trade secret owner to overcome. If, for example, the trade secret is suspected to be on a company's computer servers, a court may be unwilling to grant an order seizing the servers because of the collateral damage to the other party's business that would almost certainly occur.

Third, the trade secret owner must demonstrate that it is likely to succeed on the merits in showing that its information is a trade secret and that the accused offender misappropriated or conspired to misappropriate its trade secret. Because this is an *ex parte* proceeding, the trade secret owner will be able to present a one-sided view of the facts, but courts are aware of that tendency and tend to hold movants to a higher standard in these *ex parte* circumstances.

Fourth, the trade secret owner cannot publicize that it has requested that the court seize the information or publicize that the court has granted such an order. Clearly, Congress did not want trade secret owners to use this mechanism as a cudgel in the press, so trade secret owners need to be careful about what they say relating to any *ex parte* seizure requests or orders, or they may be barred from seeking or maintaining one.

Finally, the trade secret owner will be required to post a bond in an amount adequate to compensate the other side if the court later determines that the seizure was improper. A trade secret owner will need to think carefully about what it asks to be seized, because an overbroad seizure request could be later found to be improper and could cause substantial damages to the other side's business.

Assuming that the court grants the *ex parte* seizure order, a trade secret owner will have to act quickly in developing and litigating its case. The court must set a hearing on the merits of retaining the seized items within seven days after the order issues. At that hearing, the trade secret owner must prove the facts that supported the seizure, or the order will be dissolved. In addition, the trade secret owner cannot have access to the seized items before the hearing. Instead, the court will retain custody of the items and take measures to preserve and protect the confidentiality of the items. The court can appoint a special master to begin reviewing the seized items to make sure that they fall within the scope of the order and to return any items that fall outside of the scope.

If the court determines that the seizure was improper or unnecessary, the other side can institute an action for wrongful seizure and obtain compensatory and punitive damages, along with its attorneys' fees. So, again, trade secret owners need to think carefully about whether to seek an order and for what they should ask.

This *ex parte* seizure order is an extreme measure that has the potential to inflict serious harm to either the accused party or the trade secret owner if not done correctly. Courts are just beginning to wrestle with when and how to grant such orders. Likely, courts will be reluctant to grant them initially, except in unusual circumstances. For example, if a trade secret owner can show that a current or former employee is about to leave the country with a laptop or briefcase full of a company's trade secrets, a court may be more inclined to grant such an order to seize those items than with respect to a more traditional non-solicitation/non-compete dispute between well-established domestic companies that are within the court's jurisdiction. Also, courts may struggle with what should be seized. If the suspected trade secrets are on a company's servers, how can the court order the seizure of just the trade secrets without seizing the servers themselves? Seizing a company's servers will likely cause substantial collateral damage to the company by, for example, taking down its email accounts and eliminating access to things like its customer, billing, personnel, and payroll files. It will be difficult for a trade secret owner to show that the balance of hardships favors such an extreme type of seizure request.

As litigants begin seeking these kinds of *ex parte* seizure orders, the case law should develop quickly and provide more guidance to trade secret owners that are considering this option.

Whistleblower Protections and Notification

The DTSA also contains a provision that grants immunity from any criminal or civil liability for an unauthorized disclosure of a trade secret by any individual who discloses the trade secret to a federal, state, or local law enforcement official for the sole purpose of reporting a suspected violation of the law. Congress was concerned that the trade secret laws would discourage whistleblowers from notifying law enforcement, and it wanted to create protections that would allow individuals to disclose those kinds of concerns without the fear of facing civil or criminal penalties.

In order to improve informing employees, independent contractors, and consultants of this protection, the DTSA encourages companies to notify them explicitly of this whistleblower immunity in employee handbooks and confidentiality agreements. If a company fails to notify such an individual of this protection, the company cannot seek exemplary damages or attorneys' fees in any DTSA lawsuit against them.

Trade Secrets › page 76

Trade Secrets ❮ page 29

Therefore, companies will need to consider whether to modify their agreements and handbooks to include the required notice. In some instances, a company may decide that it is willing to forego these enhanced remedies, rather than provide the notice. But, regardless of what the company ultimately decides, it should make an informed decision on what it wants to do.

The DTSA Signals an Increased Importance of Trade Secrets

With the passage of the DTSA, companies have been given another tool to protect their intellectual property rights. While the DTSA is not revolutionary, but evolutionary, in its effect, it will give companies easier access to federal courts, along with a few new twists. We expect that the DTSA will create a more robust, predictable, and uniform body of law throughout the nation that will better enable companies to protect their valuable confidential information going forward.