Ipls PROCEEDINGS
STATE BAR OF MICHIGAN

"Defend Trade Secrets Act" Signed Into Law Effective May 11, 2016

By John M. Halan, Shareholder, Brooks Kushman PC

Volume 27 • Issue 2 • 2016

In This Issue

The Defend Trade Secrets Act of 2016 ("DTSA"), was signed into law by President Obama on May 11, 2016. The new statute creates broad private federal cause of action for trade secret misappropriation and has been hailed as "the most sweeping change to the nation's intellectual property laws in a generation or more."[1] Under DTSA, relief not generally available under prior law will now be permitted, such as ex parte seizure orders. DTSA also includes new requirements, such as the requirement that employers provide employees with notice of immunities available under DTSA in order to preserve their rights to certain relief. Accordingly, clients need to review their current policies and procedures, not only to ensure compliance with DTSA requirements, but to maximize the enforceability of trade secrets as part of their overall IP protection strategy.

Background

One goal of DTSA was to stem the growing tide of trade secret theft. A 2013 report referenced during DTSA legislation reported that losses due to trade secret theft could be measured in the hundreds of billions of dollars and in millions of jobs.[2] Foreign entities, through cyberespionage and other means, were increasingly the culprits.[3] That same year, Attorney General Eric Holder said, "There are only two categories of companies affected by trade-secret theft: those that know they've been compromised and those that don't know yet."[4]

Another goal of DTSA was to bring uniformity to trade secret civil litigation by allowing cases to be brought in federal court under DTSA if "the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce."[5] Prior to DTSA, most states had adopted the Uniform Trade Secrets Act of 1985 ("USTA"). However, various states and state courts modified or interpreted USTA provisions differently, resulting in a hodgepodge of state laws and enforcement results. While DTSA provisions largely mimic provisions of the USTA, there are differences.

While the future impact of DTSA is debatable, the need for companies to understand DTSA and to protect their trade secrets is not. This is especially true in light of the increasing theft of trade secrets. As explained below regarding specific DTSA

Continued on page 3

View from the Chair

It is my great honor to be Chair of the Intellectual Property Law Section for 2016-2017. Fall is a busy time of year for the Intellectual Property Law Section Council.

In addition to welcoming new Council members, the group plans the Section's upcoming programs: the annual Spring IP Seminar (to be held March 13, 2017 at the Kellogg Conference Center in East Lansing), and the annual IP Law Institute (co-sponsored by the Institute of Continuing Legal Education and to be held July 20-22, 2017 at the Grand Hotel on Mackinac Island).

This year, as usual, IP practitioners face the challenge of remaining current in a field that is affected by continually advancing technological issues and dramatic changes in applicable law. The Council attempts to provide value to its growing membership by presenting timely, high quality educational programs featuring distinguished speakers of national stature, representing private practice, in-house, and agency perspectives.

At the same time, we strive to present an opportunity for Section members to network and build professional relationships and lasting personal friendships. In addition to receptions at our educational programs, the Council sponsors or co-sponsors networking events (such as the reception hosted by Price Heneveld at the State Bar of Michigan Annual Meeting in Grand Rapids) and receptions for visiting representatives from the U.S. Patent and Trademark Office and other agencies (such as the recent Detroit luncheon for USPTO Deputy Director Russell Slifer).

Finally the Section actively represents Michigan's vibrant IP legal community to the public. In 2014, the Section launched the Michigan Patent Pro Bono Project in collaboration with the USPTO, part of a nationwide network of regional pro bono initiatives. The Project continues to match low income Michigan inventors with volunteer patent attorneys. We also are planning a series of presentations at Michigan law schools for students interested in IP careers. And we actively support community outreach programs through the USPTO Midwest Regional Patent Office in Detroit.

In sum, the Council works to serve its over 1,200 members across the region, and to advance the field of IP law through education, advocacy, and public outreach.

I hope you will join me in welcoming our new Council members: Angela Caligiuri (General Motors Corporation), E. Colin Cicotte (Reising Ethington PC), Matthew L. Goska (Warner, Norcross & Judd PLLC), and Mary Margaret L. O'Donnell (Blue Filament Law PLLC). And sincere thanks to both our continuing Council members, and those serving terms that expired in July: Sharon K. Brady, Tamara Ann Clark, and Eugene J. Rath.

And most of all, I would like to again acknowledge the leadership and contributions of our outgoing chair, Kristen Issacson Spano.

If you see any of these colleagues, please take a moment to thank them for volunteering to serve on the Council.

—David Berry

Continued from page 1

provisions, companies should use the enactment of the new statute as an opportunity to review their trade secret portfolios and protection practices in light of DTSA, and take action accordingly to fully protect their trade secrets.

Key Provisions

Ex Parte Seizures. The most controversial difference between UTSA and DTSA is that DTSA empowers federal courts, "in extraordinary circumstances," to issue an ex parte order – i.e. without notice to the alleged thief – "providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret." [6]

The need for such a remedy was based, at least in part, on the testimony of industry insiders. For example, one pharmaceutical company representative testified that they "often run into situations" where, after an employee has left, the company finds there has been a download of documents containing trade secrets from that employee's computer.[7] The representative testified that a seizure provision would allow the company to "go to Federal court and in one action kick out an ounce of prevention rather than worrying about a pound of cure a week or two later, when we can get the … State courts involved[.]"[8]

Accordingly, it is imperative that companies institute practices to detect trade secret misappropriation as soon as possible. Given the right set of circumstances, this will then allow them to seek and obtain an ex parte seizure order in order to minimize the damaging effects of such a theft. This is especially important at present, when trade secrets can be easily disseminated through electronic means.

Immunity Notice Requirements. Another difference between existing state law and DTSA is that under DTSA, "[a] n individual shall not be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret" in certain situations.[9] Specifically, such immunity is granted to individuals that (1) disclose a trade secret in confidence to a government official or an attorney solely to report or investigate a violation of the law, (2) disclose a trade secret to an attorney or in court proceedings in connection with a lawsuit alleging retaliation by an employer for reporting a suspected violation of the law, and (3) disclose or use a trade secret in any lawsuit filing, as long as filed under seal.

In the event such an individual is an employee, and the employer does not provide appropriate notice to such person of the availability of such immunities, that employer cannot be awarded exemplary damages (up to two times actual damages), or attorney fees, in a trade secret suit against any such person to whom such notice was not provided.[10]

Specifically, DTSA provides that for an employer to preserve its rights to exemplary damages and attorney fees, the employer "shall" provide notice to an employee of his or her immunity rights "in any contract or agreement with an employee that governs the use of trade secret or other confidential information," or by cross-referencing a policy document provided to such employee.[11] Employers should know that DTSA defines "employee" to "include[] any individual performing work as a contractor or consultant."[12] This requirement is for all agreements entered into or updated after DTSA enactment, i.e., after May 11, 2016.[13]

Accordingly, companies should take immediate steps revise all contracts or agreements (1) that relate to trade secrets or other confidential information, (2) with any employee, contractor, or consultant, and (3) that are to be entered into or updated after May 11, 2016.

Employee Mobility. Under the "inevitable disclosure doctrine" employed by many state courts, employers have been able to enjoin employees from taking a new job merely because of what they knew – without any evidence of actual misappropriation – by showing that the new job would inevitably lead to a disclosure of the employer's trade secrets. Under DTSA, a court cannot "prevent a person from entering into an employment relationship, and that conditions placed on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows."[14]

Given the increased right of employment mobility provided under DTSA, it is important that companies revisit their employee practices. Not only should employee agreements be reviewed, companies should institute appropriate employee exit strategies. For example, reminding a departing employee of their trade secret obligations should be part of every exit interview, preferably coupled with a written acknowledgement of such obligations signed by the departing employee. As another example, the employee's next employer should be contacted in writing and warned that the employee is restricted from disclosing or using trade secrets relating to certain areas of knowledge such as manufacturing, formulas, customers, etc. This prevents the next employer from later claiming innocent use of any such trade secrets.

DTSA Does Not Preempt State Law. DTSA specifically provides that it does not preempt state trade secret law. Accordingly, DTSA will add to the complexity of trade secret litigation. As an example, a plaintiff may now choose to bring trade secret civil litigation under DTSA, under state law, or both —depending upon which strategy is the most advantageous.

Further, because decisions under DTSA will be made by federal district court judges in each state, it can be presumed that DTSA provisions will not only be interpreted differently between such judges, but that such judges may be pre-disposed or influenced by the pre-existing state laws and precedents of their jurisdiction.

Accordingly, companies should work with legal counsel in determining how differences between existing state laws and DTSA may work to their advantage. For example, DTSA defines what constitutes a trade secret differently than, and arguably broader than, the definition provided under state law. Accordingly, companies may need to reevaluate their confidential information, and whether it should be guarded under trade secret precautions.

More importantly, state trade secret law under UTSA requires that in order confidential information to be maintained as a trade secret, it must be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[15] DTSA, on the other hand, requires that the "owner thereof has taken reasonable measures to keep such information secret."[16] While it is unlikely that DTSA will be interpreted to require different measures to keep such information secret, this is a good time for companies to revisit the measures they do use. This is critical because confidential information qualifies as a trade secret only if appropriate measures are taken to keep it secret, such as by (1) restricting access to such information, (2) using contracts to restrict employees and others from using or disclosing such information, and (3) providing notice to others of their trade secret obligations. Examples of each would be (1) using passwords to restrict electronic access to trade secrets, (2) using appropriate nondisclosure agreements, and (3) again, instituting employee exit interview strategies in order to place exiting employees, and their future employers, on notice of their trade secret obligations.

Practice Points

In enacting DTSA, Congress recognized the ever-increasing importance of trade secrets in the competitive global marketplace. DTSA also reflects a recognition of the limitations inherent in using patents to protect certain key intellectual property; including continuing uncertainties concerning the patent eligibility of some technologies. DTSA is a significant attempt to address the uneven application of trade secret protection under state laws and the difficulty in enforcing trade secrets in foreign venues.

Given the extreme value of trade secrets, and the growing threat of trade secret theft, it would behoove businesses to reassess and audit their trade secret protection practices in light of DTSA, and take appropriate steps to protect those trade secrets. In order to get the most out of the new enforcement options in DTSA, clients must make sure that their policies and procedures meet the requirements of the Act, and also serve to maximize the protection of trade secrets and other IP assets.

This includes, for example, revising all contracts or agreements relating to trade secrets or other confidential information with any employee, contractor, or consultant to provide the notices required by DTSA. In addition, companies should evaluate their policies concerning restrictive covenants and non-competition agreements to ensure that they are appropriate and meet the requirements of state law. Finally, clients should audit their current practices for safeguarding trade secrets and confidential information to make sure that the information is protected from recent advances in cyberespionage, and also to enhance the ability to win in litigation in the event that, despite those precautions, trade secrets are misappropriated or fall into the hands of a competitor.

About the Author

John Halan *is the head of Brooks Kushman's trade secrets group. His practice focuses on intellectual property litigation, including patent, trade secret and related commercial litigation. With over 25 years of experience, he has represented clients in a broad range of industries and has considerable expertise handling matters before state and federal courts and the USPTO Patent Trial and Appeal Board, including inter partes reviews and appeals. Halan holds a Juris Doctor from Wayne State University Law School and a Bachelor of Science in Engineering from Michigan State University where he graduated with high honors. He is also a licensed engineer.*

Endnotes

1 Maxwell Goss, *What the Defend Trade Secrets Act Means for Trade Secret Defendants*, PatentlyO, (May 5, 2016), *http://patentlyo.com/?s=defend+trade+secrets+act.*

2 The IP Commission, *Report Of The Commission On The Theft Of American Intellectual Property*, 11 (May 2013), *http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.*

3 *Id.* at 3.

4 S. Rep. No. 114-220, at 2 (2016).

5 18 U.S.C. § 1836(b)(1); DTSA § 2(a).

6 18 U.S.C. § 1836(b)(2)(A)(i); DTSA § 2(a).

7 *Economic Espionage And Trade Secret Theft: Are Our Laws Adequate For Today's Threats? Before S. Comm. on the Judiciary*, 113th Cong. (2014) at 15 (statement of Douglas K. Norman, Eli Lilly & Co.)

8 *Id.*

9 18 U.S.C. § 1833(b); DTSA § 7.

10 18 U.S.C. § 1833(b)(3); DTSA § 7.

11 *Id.*

12 18 U.S.C. § 1833(b)(4); DTSA § 7.

13 DTSA § 2.

14 18 U.S.C. § 1836(b)(3)(A); DTSA § 2.

15 UTSA § 1(4)(ii).

16 18 U.S.C. § 1839(3)(B); DTSA § 2.

Enfish and *TLI*: A Study of the CAFC's Recent Section 101 Opinions

By Stephen Marshall, Fish & Richardson

This article originally appeared on the Fish Litigation Blog at *http://www.fr.com/fish-litigation/* and is used with permission from the author.

Like a ray of light at the end of a long dark tunnel, the Federal Circuit's recent reversal of a determination of patent ineligibility in *Enfish, LLC v. Microsoft Corp.*, __ F.3d (Fed. Cir. May 12, 2016) (Hughes, J.) offered patentees facing *Alice* proceedings a glimmer of hope. Reaction by the patent bar was swift. Notices of additional authority and requests for reconsideration were submitted to district courts around the country. Commentary has already been posted to the internet hailing *Enfish* as a long-awaited clarification of *Alice*. The USPTO even issued a Memorandum of guidance regarding *Enfish* to the Examining Corps.[1]

However, less than a week after *Enfish*, the Federal Circuit, with Circuit Judge Hughes again as author, issued an opinion regarding *In re TLI Communications LLC Patent Litigation*, F.3d (Fed. Cir. May 17, 2016), in which the court appeared to return to a pre-*Enfish* approach. The *TLI* opinion addresses *Enfish* and offers a narrow distinction between the two cases. It remains to be seen whether the carve-out announced in *Enfish* is sound and will withstand scrutiny, or whether *Enfish* will bring more confusion than clarification to the *Alice* landscape.

The Supreme Court's *Alice* decision gave little specific guidance to district courts on applying its two-step eligibility test. At the Federal Circuit Judicial Conference in Washington, D.C. in April, Judge Gilstrap commented that "[i]t's a challenge to interpret the court's analysis and apply it faithfully."[2] After several years in which software patents have routinely been deemed patent ineligible, patentees hope that *Enfish* will provide much needed direction about the application of *Alice*. However, when *Enfish* and *TLI* are read together, that proposition appears in doubt.

Enfish

In *Enfish*, the plaintiff below asserted U.S. Patent Nos. 6,151,604 and 6,163,775, both of which are directed to a particular logical model for a computer database. In contrast to a relational database model that uses relationships between multiple tables to store various fields of information, the asserted patents disclosed a self-referential model in which all data entities are in a single table, and the column definitions are provided by the rows. (*Enfish Slip op.* at 2-5.) An example of such a self-referential table is shown below.

SELF-REFERENTIAL TABLE

ID	Type	Title	Label	Address	Employed by (#4)	Author	Email (#5)
#1	DOCUMENT	PROJECT PLAN		C:\WORD\ PROJ.DOC		#2	
#2	PERSON		SCOTT WLASCHIN		#3		
#3	COMPANY		DEXIS	117EAST COLORADO			
#4	FIELD		EMPLOYED BY				
#5	FIELD		EMAIL				

(*Id.* at 7.) According to the asserted patents, the self-referential model allows for faster searching, more flexibility in configuring the database, and more effective storage of images and unstructured text. (*Id.*) The district court determined that the asserted claims of these patents, however, were not patent eligible under § 101 because they were directed to the abstract concept of "organizing information using tabular formats." (*Id.* at 14.)

On review, the Federal Circuit first laid the groundwork for its analysis with the principals that *Alice* "plainly contemplates that the first step of the inquiry is a meaningful one, *i.e.*, that a substantial class of claims are *not* directed to a patent-ineligible concept" (*id.* at 10 (emphasis in original)), and that claims are to be evaluated under Step One "based on whether 'their character as a whole is directed to excluded subject matter'" (*id.* (quoting *Internet Patents Corp. v. Active Network, Inc.*, 790 F.3d 1343, 1346 (Fed. Cir. 2015))). Both of these statements are encouraging for patentees but are simply recitations of existing law.

The Federal Circuit next interpreted *Alice*'s Step One analysis in the context of computer-related technology to determine that it is "relevant to ask whether the claims are directed to an improvement to computer functionality versus being directed to an abstract idea, even at the first step of the *Alice* analysis." (*Id.* at 11.) Underlying this conclusion is that the court "do[es] not read *Alice* to broadly hold that all improvements in computer-related technology are inherently abstract" nor that "claims directed to software, as opposed to hardware, are inherently abstract and therefore only properly analyzed at the second step of the *Alice* analysis." (*Id.*)

The Federal Circuit's reasoning in *Enfish* appears to create a new inquiry for computer-related technology under Step One: "whether the focus of the claims is on the specific asserted improvement in computer capabilities … or, instead, on a process that qualifies as an 'abstract idea' for which computers are invoked merely as a tool." (*Id.*) Turning to the self-referential database model at issue, the court held that the focus of the asserted claims is "on an improvement to computer functionality itself, not on economic or other tasks for which a computer is used in its ordinary capacity." (*Id.* at 12.)

The court's conclusion was bolstered by the disclosed benefits of the model— increased flexibility, faster search times, and smaller memory requirements. (*Id.* at 15.) Finally, the court distinguished (patent eligible) claims directed to a specific improvement in computer functionality with (patent ineligible) claims that recite use of an abstract mathematical formula on any general purpose computer, recite a purely conventional computer implementation of a mathematical formula, or recite generalized steps to be performed on a computer using conventional computer activity. (*Id.* at 17.)

On its face, the *Enfish* opinion is a boon for patentees of software-related technologies because it appears to create a new safe zone for "improvements in computer functionality." However, is this carve-out as clear and sound as it may seem? The first clue in answering that question may come from the *TLI* opinion, issued just days after and from the same authoring Judge as *Enfish*.

TLI

The fate of U.S. Patent No. 6,038,295, in the *TLI* opinion, is quite different from that of the patents in *Enfish*: "the ['295 patent] claims no more than the abstract idea of classifying and storing digital images in an organized manner." Accordingly, *TLI* affirmed the district court's determination that the patent fails to claim patent-eligible subject matter under § 101. (*TLI Slip op.* at 3.)

The patent-in-suit in *TLI* related to "an apparatus for recording of a digital image, communicating the digital image from the recording device to a storage device, and to administering the digital image in the storage device." The claimed invention was intended to address challenges in organizing a large database of digital images stored on a computer. The goal of the inventors was to administrate and archive the "digital images simply, fast and in such way that the information therefore may be easily tracked" using manually or dynamically assigned "classification data." (*Id.* at 3-4 (citing the '295 patent).)

Under *Alice* Step One, the Federal Circuit first observed that "representative claim 17 is drawn to the concept of classifying an image and storing the image based on its classification," but then unexpectedly appears to move into the Step Two analysis in the very next sentence, stating: "the specification makes clear that the recited physical components merely provide a generic environment in which to carry out the abstract idea of classifying and storing digital images in an organized manner." (*Id.* at 7-8.) Returning to Step One, the *TLI* opinion next recites the carve-out of *Enfish* but concludes that "the [TLI] claims here are not directed to a specific improvement to computer functionality." (*Id.* at 8.) The court reasoned that the claims of the asserted patent are instead "directed to the use of conventional or generic technology in a nascent but well-known environment." (*Id.*)

Still within the context of its Step One analysis, the court further criticized the '295 patent for "fail[ing] to provide any technical details for the tangible components" and "predominately describ[ing] the system and methods in purely functional terms" rather than "describ[ing] a new telephone, a new server, or a new physical combination of the two." (*Id.* at 9.) The opinion also highlights that the telephone and server components of the asserted claims are described in the specification as being well-known. The court concluded that "the focus of the patentee and of the claims was not on an improved telephone unit or an improved server." (*Id.* at

9-10.) For all these reasons, the claims of the '295 patent were deemed directed to an abstract idea.

Turning to its Step Two analysis, the court held that none of the recited physical components add an inventive concept sufficient to bring the abstract idea into the realm of patentability. (*Id.* at 11.) Having failed both analytical steps of Alice, the asserted claims were affirmed to be patent ineligible.

Analysis

Despite the attempted harmonizing discussion of *Enfish* in *TLI*, the latter exposes several inconsistencies between the opinions as well as potential flaws in the reasoning of *Enfish*. As an initial matter, the Federal Circuit's descriptions of the claimed technologies in each of the opinions share similarities in areas that impacted the legal analysis. Each involved a database implementation on a commodity computer. Also, the benefits of each purport to include increased search speed and dynamic configuration of data files. Additionally, the disclosure of each was largely functional with little to no emphasis on new physical components.

The court's treatment of these apparent factual similarities could not have been more different. In *Enfish*, the court found that the self-referential model led to an "improvement in computer capabilities" but the claimed invention did not give the computer more total memory, or a processor with greater clock speed, or a faster bussing architecture.

The self-referential model creates a logical data structure that allows for faster results to be returned in comparison to other logical database models. This represents an algorithmic improvement rather than an improvement in the capabilities of the physical hardware on which the algorithm executes. For example, there are numerous algorithms for sorting a collection of elements, and on average, a bucket sort performs substantially better than a selection sort. Executing a bucket sort rather than a selection sort on a particular computer does not change the fundamental capabilities of that computer; the computer executes the same number of operations per unit time in either scenario. Rather, the performance benefit is attributable to the algorithm. The *Enfish* court, however, found that the self-referential model indeed provided an "improvement in computer capabilities."

In contrast, the *TLI* court lambasted the claimed image database using classification data for failing to improve the recited telephone unit or server. The *TLI* opinion highlighted that "the server is described simply in terms of generic computer functions such as storing, receiving, and extracting data." (*TLI Slip op.* at 9.) However, the computer on which the self-referential database of *Enfish* is configured, would also merely receive, store, and extract data—this is the fundamental role of a computer running a database.

The Federal Circuit also found support for its analysis in *Enfish* in the alleged benefits of the self-referential model over existing solutions. The court emphasized faster search times and flexibility from not needing programmer pre-configuration. The TLI invention claimed to offer similar benefits by providing a classification based indexing solution and automated assignment of classifications. However, the court was unmoved by these very same benefits in the *TLI* analysis, instead finding that, for example, "attaching classification data, such as dates and times, to images for the purpose of storing those images in an organized manner is a well-established basic concept." (*TLI Slip op.* at 11 (internal quotations omitted).) In so doing, the Federal Circuit appears to have taken the same approach in *TLI* as it criticized the district for taking in *Enfish*: "the district court oversimplified the self- referential component of the claims and downplayed the invention's benefits." (*Enfish Slip op.* at 15.)

The *Enfish* opinion also was notably open-minded in assessing the functional description of the claimed invention, recognizing that "[m]uch of the advancement made in computer technology consists of improvements to software that, by their very nature, may not be defined by particular physical features but rather by logical structures and processes." (*Id.* at 17-18.) The *Enfish* opinion never states whether the invention provided technical details of the tangible components or described "a new computer." To the contrary, the '604 Enfish patent describes the involved computer as having an "(I/O) circuit 22" and "a central processing unit (CPU) 24 coupled to the I/O circuit 22 and to a memory 26," and that "[t]hese elements are those typically found in most computers and, in fact, computer 23 is intended to be representative of a broad category of data processing devices." ('604 patent, col. 5:25-33.) This is hardly a "new computer." The *TLI* opinion took a different view of the database system disclosure in the '295 patent. The court criticized the disclosure for failing to provide technical details about physical features or describing "a new server," and instead focusing on "purely functional terms." (*TLI Slip op.* at 9.)

Not only is the different evaluation of similar evidence notable, but so too is the court's use of the specification. In *Enfish*, the court pointed out that the Step One analysis should look to the claims as a whole to determine if they are directed to eligible subject matter. Having reached that conclusion in *Enfish*, the court then found that the specification added support for its conclusion. In contrast, the *TLI* court looked first to the specification disclosure to determine that the claims were not directed to patent eligible subject matter. (*Id.* at 7-8.)

Observations

Given the comparisons and contrasts between *Enfish* and *TLI*, it seems that the former was inconsistently, if not incorrectly, decided. Setting aside the *Enfish* carve-out for a moment, had the Federal Circuit applied the same analysis from *TLI* in the *Enfish* case, the Enfish patents should not

have been found subject matter eligible. As such, it was the court's "improvement in computer capabilities" carve-out that saved the Enfish patents.

Looking more closely at the supposed clarification to the *Alice* Step One analysis—"improvement in computer capabilities"—it seems nothing more than a question of novelty rather a determination of abstractness, which is what Step One is meant to reach. The word "improvement" suggests novelty. Indeed, the Federal Circuit highlighted that the Enfish self-referential model "functions *differently than conventional* database structures" and is "directed to an *improvement if an existing* technology." (*Enfish Slip op.* at 15 (emphasis added).) This tendency to draw notions of novelty and obviousness into the Step One analysis is a core problem with the *Alice* framework in the context of software-related technologies, and may indicate the lack of a clear or appropriate test in that context. The blurred lines of abstractness and novelty also manifest in the conflation of Step One and Step Two, as is seen in the *TLI* opinion.

Where does the clarification of *Enfish* leave the patent bar? For the time being, *Enfish* may represent a safe-harbor for patent eligibility of software patent claims. It will almost certainly add to the burden of accused infringers of such claims that seek relief under § 101, and demand even more close calls from district courts weighing the issue. The required notice function of software patent claims, however, will continue to fail the public. Between the endpoints of firmware that makes a machine functional and software that does little more than use a computer as a calculator lay applications that, based on *Enfish* and *TLI*, may or may not be patent eligible.

One potential solution for software related technologies is a § 101 test that simply examines whether the claimed invention is a technical solution within a technical field. This is similar to the standard set forth in *Diamond v. Diehr*, 450 U.S. 175 (1981). Such a determination should exclude pure business methods and execution of a mathematical formula on a generic computer. Thereafter, §§ 102, 103, and 112 would still act to filter unpatentable claims, but backed by a robust jurisprudence with ample guidance for application. Under this or a similar approach, *Enfish* and *TLI* may have reached the same results but without an inconsistency in reasoning between them.

Conclusion

Enfish likely represents yet another notable piece in the yet-to-be- solved puzzle of patent eligibility of software patent claims. Whether it will provide much needed clarification or further muddy the *Alice* framework remains to be seen. If nothing else, *Enfish* amplifies current concerns from the patent bar and bench about how to apply *Alice* in this context. Indeed, the *Enfish* opinion itself states that the "Supreme Court has not established a definitive rule to determine what constitutes an 'abstract idea' sufficient to satisfy the first step of the *Mayo/Alice* inquiry." (*Slip op.* at 9.) If not *Enfish*, perhaps its progeny could be headed for the Supreme Court to provide such a definitive rule.

Endnotes

1 *See* "Recent Subject Matter Eligibility Decisions (*Enfish, LLC v. Microsoft Corp.* and *TLI Communications LLC v. A.V. Automotive, LLC*)" at *http://www.uspto.gov/sites/default/files/documents/ieg-may-* 2016_enfish_memo.pdf.

2 *See* "Gilstrap, Stark Say Alice, AIA 'Sea Change' Means More Work," Ryan Davis, Law360 (April 11, 2016) at *https://www.law360.com/articles/783102*.

The Defend Trade Secrets Act: Some Practical Considerations

By Kenneth Kuwayti, Bryan Wilson, and Christian Andreu-von Euw, Morrison Foerster

President Obama recently signed the Defend Trade Secrets Act (DTSA or the "Act"), which created a new federal cause of action for trade secret misappropriation effective immediately.

The DTSA establishes federal jurisdiction for claims brought under the Act, which will now provide trade secret plaintiffs with the option to sue in federal court and bring with it the potential for a more unified body of federal law.

Although trade secret theft has been a federal crime since 1996, civil claims for trade secret misappropriation were almost always governed by state law.[1] As a result, although plaintiffs who could establish diversity or concurrent jurisdiction could file trade secret cases in federal court, other plaintiffs were limited to state court. Nearly every state has adopted some variant of the Uniform Trade Secrets Act (UTSA). Its title notwithstanding, the UTSA suffered from a perceived lack of uniformity due to the many variations in the state statutes adopting it. Because the Act does not preempt state trade secret law claims, the option to proceed under state law, and in state court, will remain.

What's New

Employers Should Update Employment Agreements to Provide DTSA Notices

Only one provision of the DTSA requires immediate action: the Act includes a whistleblower clause that provides immunity for disclosure of trade secrets to government officials for the sole purpose of reporting violations of the law.[2] Employers must give notice of that immunity "in any contract or agreement with an employee that governs the use of a trade secret or other confidential information."[3] Employers who do not do so cannot recover punitive damages or attorneys' fees that may otherwise be available under the Act.

Employers should consider addressing this clause in current policies regarding trade secret information (or establishing such policies if they do not exist) and reviewing existing employment, non-disclosure, proprietary information and invention assignment, and other agreements that govern the use of a trade secret or other confidential information to ensure compliance with the DTSA. For example, employers could insert a cross- reference to a compliant policy, or the following language into those agreements:

> 18 U.S.C. § 1833(b) states:
>
> > "An individual shall not be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret that—(A) is made—(i) in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney; and (ii) solely for the purpose of reporting or investigating a suspected violation of law; or (B) is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal."
> >
> > Accordingly, the Parties to this Agreement have the right to disclose in confidence trade secrets to Federal, State, and local government officials, or to an attorney, for the sole purpose of reporting or investigating a suspected violation of law. The Parties also have the right to disclose trade secrets in a document filed in a lawsuit or other proceeding, but only if the filing is made under seal and protected from public disclosure. Nothing in this Agreement is intended to conflict with 18 U.S.C. § 1833(b) or create liability for disclosures of trade secrets that are expressly allowed by 18 U.S.C. § 1833(b).

International Trade Secrets Disputes and Foreign Competition

The DTSA imposes reporting requirements to address the internationalization of trade secret disputes. The Act requires the Attorney General to prepare biannual reports detailing, among other things, the scope of theft of American trade secrets occurring outside of the United States, the extent to which those thefts are sponsored by foreign governments, a breakdown of the trade secret protections in each of the United States' trading partners, and specific recommendations to the executive and legislative branches for reducing trade secret theft and protecting American companies. The first report is due in one year.

The reporting requirement may lead to further amendments to the Act designed to provide further protections to United States companies. The reports could also lead to pressure being exerted on certain trading partners and could eventually lead to efforts to harmonize trade secrets law among international trading partners.

Standing Requires Ownership

Unlike the trade secrets statutes in some states, the DTSA allows an "owner of a trade secret" to bring a civil action under the Act. The California statute, for example, does not have such a stringent requirement, and California courts have held that it does not require a plaintiff to be a current owner of a trade secret.[4]

New Disclosure Protections (for All Federal Suits)

The DTSA prohibits district courts from "authoriz[ing] or direct[ing] the disclosure of any information [a trade secret] owner asserts to be a trade secret unless the court allows the owner the opportunity to file a submission under seal that describes the interest of the owner in keeping the information confidential."[5] This provision—which is not expressly limited to DTSA cases—may have broader applicability and could lead to more sealed filings and orders.

Ex Parte Seizure Orders

The DTSA adds an important remedy not found in the Uniform Trade Secrets Act: it provides for ex parte orders "providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret."[6] This has been one of the most publicized new provisions of the Act, simultaneously lauded and vilified, depending on your point of view.

In fact, this procedure is likely to be employed infrequently, because the prerequisites for the issuance of a seizure order order are lengthy and exacting. To issue such an order, a court must find all of the following: (i) another form of equitable relief would be inadequate because the party to be enjoined would evade, avoid, or otherwise not comply; (ii) immediate and irreparable injury will occur if such seizure is not ordered;

(iii) the harm to the applicant outweighs the interests of the party to be enjoined and substantially outweighs potential harm to third parties; (iv) the applicant is likely to succeed on the merits; (v) the party to be enjoined has actual possession of the trade secret; (vi) the application describes the matter to be seized with reasonable particularity; (vii) the party to be enjoined would destroy, move, hide, or otherwise make such matter inaccessible to the court; and (viii) the applicant has not publicized the requested seizure.[7] An ex parte seizure order must include those detailed findings of fact and law and a number of other requirements, such as instructions that provide for the narrowest seizure of property necessary, detailed guidance to law enforcement (including permissible hours of seizure and the directions about the amount of force authorized), and instructions on protecting the seized property from disclosure.[8] The burden imposed on plaintiffs preparing these applications, and courts reviewing them, will be substantial.

The DTSA provides a number of special procedures for handling seized material, including the use of a special master to locate and isolate the seized material and the potential use of encryption to secure the seized material. The use of special masters could be an attractive option for overburdened courts faced with administering these procedures.

What Stayed the Same (in California and Other States)

No Preemption

The DTSA does not preempt states' trade secrets acts or any other state laws.[9] Accordingly, state law causes of action should remain largely unchanged.

Similarity to Uniform Trade Secrets Act

The DTSA is modeled on the Uniform Trade Secrets Act, which is also the model for the trade secret statutes in California[10] and other states. Therefore, the elements of a DTSA misappropriation claim are similar to the elements of state law trade secret claims.[11] Given the many variations in UTSA-based statutes, however, there are significant differences that vary from state to state.

The DTSA provides the same remedies as the California Uniform Trade Secrets Act and most UTSA states, plus the ex parte seizure remedy.[12] It also has the same three-year statute of limitations as California.[13] Importantly, like the UTSA, the DTSA states that a continuing misappropriation constitutes a single claim of misappropriation and thereby precludes arguments that each new act of misappropriation restarts the statute of limitations.

The Act Does Not Adopt the Inevitable Disclosure Doctrine

Under the inevitable disclosure doctrine, "a plaintiff may prove a claim of trade secret misappropriation by demonstrating that [a] defendant's new employment will inevitably lead [the defendant] to rely on the plaintiff's trade secrets."[14] The doctrine has been rejected in California and other states because it "'creates a de facto covenant not to compete' and 'runs[s] counter to the strong public policy in California favoring employee mobility.'"[15]

The inevitable disclosure doctrine was a topic of significant discussion in legislative hearings for the DTSA, and the DTSA is designed to strike a careful balance to ensure that the DSTA does not introduce the inevitable disclosure doctrine to states that have rejected it. The DTSA expressly forbids injunctions that "conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business"[16] or limit employment based "merely on the information the person knows." [17] The lack of an inevitable disclosure claim in the DTSA is consistent with the White House's recent report on Non-compete Agreements, which "address[es] the potentially high costs of unnecessary non-competes to workers and the economy."[18]

What Remains to be Seen

There are many issues that will be determined as jurisprudence under the DTSA develops. To what extent will federal courts apply the law of the state in which they are sitting? Will federal courts become the default venue for civil trade secret claims, or will plaintiffs prefer to proceed in state courts, which are sometimes perceived as a more plaintiff-familiar venues? We address a few specific issues below.

The Act's Impact on Section 2019.210 Is Uncertain

California Code of Civil Procedure Section 2019.210 requires a trade secret plaintiff to identify its claimed trade secrets with "reasonable particularity" before commencing discovery.[19] The DTSA has no such express requirement.

One court has noted that section 2019.210 gives defendants "strategic and tactical advantages . . . not only because plaintiffs must 'go first,' which allows defendants to tailor their defense to plaintiffs' disclosure, but also because there is often significant delay and cost" due to disputes about the adequacy of a Section 2019.210 disclosure.[20] Before the DTSA, federal courts hearing California trade secrets act claims split on whether Section 2019.210 applies in federal court. Some courts have chosen to follow the procedure voluntarily, or have found that Section 2019.210 is substantive law that applies in federal court and that it is "generally consistent with Rule 26's requirements of early disclosure of evidence relevant to the claims at issue and the Court's authority to control the timing and sequence of discovery in the interests of justice."[21] Other courts, however, have found that Section 2019.210 is a procedural requirement that does not apply in federal court.[22]

As the DTSA has no express equivalent to Section 2019.210, a plaintiff filing a DTSA claim can argue that it need not separately identify its claimed trade secrets with

"reasonable particularity" beyond what might be required to properly plead its claims. The text of Section 2019.210 arguably supports this position, as it expressly limits the statute's reach to "trade secret [allegations] under the [California] Uniform Trade Secrets Act."[23] Defendants can counter, however, that the statute was drafted before the DTSA existed (and the legislature intended the statute to apply to all trade secret claims). Defendants also can rely on opinions holding that "section 2019.210 is not 'cause of action' specific [but instead] refers to any 'action,' *i.e.* the entire lawsuit, 'alleging . . . misappropriation of a trade secret.'"[24]

The Act May Not Impact the Exclusive Nature of a Trade Secret Claim

The UTSA provides for preemption of other civil causes of action based upon the misappropriation of a trade secret. California's trade secrets act, for example, "provides the exclusive civil remedy for conduct falling within its terms, so as to supersede other civil remedies 'based upon misappropriation of a trade secret.'"[25] Courts therefore routinely dismiss related tort claims[26] such as business interference, conversion, and negligence that are based on the same factual allegations as a trade secrets claim.[27] One federal court has recently held that the California trade secrets act preempts non-contract claims that "rely on the alleged misappropriation of Confidential Information" even if no trade secret claim is pled.[28]

Because the Act does not preempt state law claims, a plaintiff may argue that it may file a DTSA claim and also pursue other tort claims based on the same facts. Such tort claims based on state law are arguably superseded by the California trade secrets act's exclusivity even if no California trade secrets act claim is asserted, but it remains to be seen how the courts will resolve this issue.

Conclusion

The DTSA ushers in a new era in trade secret law by providing for a federal civil cause of action for trade secret misappropriation, and bringing trade secret law in line with its federal IP cousins. The Act strikes a careful balance to preserve many of the important elements of state law. It remains to be seen how federal jurisprudence will develop and whether federal court will now become trade secret plaintiffs' new forum of choice.

To Contact the Authors

Kenneth Kuwayti *- (650) 813-5688 and kkuwayti@mofo.com*
Bryan Wilson *- (650) 813-5603 and bwilson@mofo.com*
Christian Andreu-von Euw *- (858) 720-5126 and christian@mofo.com*

Endnotes

1 There are a few notable exceptions. *See, e.g., TianRui Grp. Co. v. Int'l Trade Comm'n*, 661 F.3d 1322, 1327 (Fed. Cir. 2011).

2 18 U.S.C. § 1833(b)(1).

3 18 U.S.C. § 1833(b)(3)(A).

4 *See Jasmine Networks, Inc. v. Super. Ct.*, 180 Cal. App. 4th 980, 986 (2009).

5 18 U.S.C. § 1835(b).

6 18 U.S.C. § 1836(b)(2)(A)(i).

7 18 U.S.C. § 1836(b)(2)(A)(ii).

8 18 U.S.C. § 1836(b)(2)(B).

9 18 U.S.C. § 1836(f).

10 California Uniform Trade Secrets Act. (Cal. Civ. Code § 3426, *et seq.*).

11 *Compare* 18 U.S.C. § 1839(3)-(6) *with* Cal. Civ. Code § 3426.1.

12 *Compare* 18 U.S.C. § 1836(b)(3) to Cal. Civ. Code § 3426.2-3426.4.

13 18 U.S.C. § 1836(d).

14 *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262, 1269 (7th Cir. 1995).

15 *Whyte v. Schlage Lock Co.*, 101 Cal. App. 4th 1443, 1463 (2002) (quotation omitted) ("Lest there be any doubt about our holding, our rejection of the inevitable disclosure doctrine is complete.").

16 18 U.S.C. § 1836(b)(3)(A)(i)(II).

17 18 U.S.C. § 1836(b)(3)(A)(i)(I).

18 See https://www.whitehouse.gov/sites/default/files/non-competes_report_final2.pdf

19 Cal. Civ. Proc. Code § 2019.210.

20 *Perlan Therapeutics, Inc. v. Super. Court*, 178 Cal.App. 4th 1333, 1353 (2009).

21 *See, e.g., Soc. Apps, LLC v. Zynga, Inc.*, No. 4:11-CV-04910 YGR, 2012 WL 2203063, at *2 (N.D. Cal. June 14, 2012).

22 *See, e.g., Funcat Leisure Craft, Inc. v. Johnson Outdoors, Inc.*, No. CIV. S-06-0533, 2007 WL 273949, at *3 (E.D. Cal. Jan. 29, 2007).

23 Section 2019.210 applies "[i]n any action alleging the misappropriation of a trade secret under the Uniform Trade Secrets Act (Title 5 (commencing with Section 3426) . . . of the [California] Civil Code)."

24 *Advanced Modular Sputtering, Inc. v. Super. Court*, 132 Cal. App. 4th 826, 834 (2005) (holding that Section 2019.210 suspends discovery into all claims related to a trade secret claim).

25 *See Silvaco Data Sys. v. Intel Corp.*, 184 Cal. App. 4th 210, 236 (2010)(quoting Cal Civ Code § 3426.7), *as modified on denial of reh'g*, No. H032895, 2010 Cal. App. LEXIS 771 (May 27, 2010) *overruled in non-pertinent part, Kwikset Corp. v. Super. Court*, 51 Cal. 4th 310 (2011).

26 The CUTSA, like the UTSA, expressly allows related contract claims. *See* Cal. Civ. Code § 3426.7; *see also Angelica Textile Servs., Inc. v. Park*, 220 Cal. App. 4th 495, 506 (2013), *as modified on denial of reh'g*, No. D062405, 2013 Cal. App. LEXIS 908 (Nov. 7, 2013).

27 *See, e.g.*, *Callaway Golf Co. v. Dunlop Slazenger Grp. Americas, Inc.*, 318 F. Supp. 2d 216, 220 (D. Del. 2004).

28 *Total Recall Techs. v. Luckey*, No. C 15-02281 WHA, 2016 WL 199796, at *8 (N.D. Cal. Jan. 16, 2016).

Five Things to Know About the Defend Trade Secrets Act

By Peter J. Toren, Weisbrod, Matteis & Copley

On April 27, 2016, Congress passed the Defend Trade Secrets Act ("DTSA"), which President Obama is scheduled to sign later today. The DTSA extends the current Economic Espionage Act of 1996 ("EEA), which criminalizes trade secret thefts, to the civil arena. This means for the first time, trade secret owners can now bring suits in federal district courts, without having to resort to another basis for jurisdiction, such as the ill-fitting Computer Fraud and Abuse Act. While not without critics, the DTSA is a major step forward in the protection of intellectual property in the United States, not least because federal law now fully recognizes four types of intellectual property (patents, copyrights, and trademarks). This article highlights five important things that every trade secret owner should know, which includes almost every company in the U.S.

1. The DTSA Provides for Civil Action in Federal Court

The DTA will amend the Economic Espionage Act of 1996 to provide that: "An owner of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." Thus, the DTSA provides for as broad a basis for jurisdiction as is permitted under the Commerce Clause of the Constitution.

Indeed, Congress amended the EEA in 2012 to include identical language for criminal violations in response to an appellate court decision that held that the use of a trade secret did not meet the then requirement that a trade secret must be "related to a product or service used in or intended for use in" commerce. This means that under the DTSA, for example, that a federal court could have jurisdiction over a claim of the misappropriation of a trade secret that used exclusively on an internal basis by the victim or one that is related to a product or service that is in the development stage so long as the trade secret is related to a product that is intended for use in interstate commerce. There are very few trade secrets that would seemingly fail to meet this requirement.

2. Misappropriation

Misappropriation under the DTSA, in general, includes: without permission (A) obtaining a trade secret that was knowingly obtained through improper means or (B) disclosing or using a trade secret without knowing either (1) that it is a trade secret or (2) that it was obtained through improper means. The "improper means" include "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means." However, misappropriation does not include "reverse engineering, independent derivation, or any other lawful means of acquisition." These potential defenses are consistent with the existing body of trade secret law under state laws and the EEA.

The definition of "misappropriation" is almost identical to the definition of "misappropriation" under the UTSA, but differs in several key respects from the definition of "misappropriation under the EEA. For example, the EEA does not explicitly provide that the "disclosure" of a trade secret

is a violation. There have been no reported cases under the EEA as to whether mere disclosure meets the definition of misappropriation, and it will be interesting to see whether courts treat what constitutes misappropriation differently under the EEA as compared to the DTSA.

3. The Definition of a "Trade Secret" is Generally Broader than Under State Law

The DTSA adopts the EEA's broad definition of a trade secret to mean "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 if—(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the another person who can obtain economic value from the disclosure or use of the information." In short, almost every type of information can qualify as a trade secret under the EEA so long as: (1) the information is actually secret; (2) the owner took reasonable measures to maintain that secrecy; and (3) independent economic value is derived from that secrecy. By comparison the UTSA identifies, by way of example, eight specific types of trade secret information; "formula, pattern compilation, program device, method, technique or process." Whether this difference will matter remains to be seen.

A second and potentially more important difference is that the EEA's definition, and now the DTSA's definition of trade secrets encompasses information in any form, "whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing." While, the meaning of this language has not been addressed in the more 20 years since the enactment of the EEA, the language suggests that information "stored" only in an individual's memory can be the subject of a civil claim for theft of trade secrets.

Finally, the EEA also previously provided that a trade secret must "derive independent economic value … from not being generally known to, …the public." Under this standard, information that was known in an industry but was not known to the public could theoretically still meet the definition of a trade secret. Without deciding this issue, an appellate court in an EEA case used the example of "Avogadro's number" to illustrate the difference between "public" and "person who can obtain economic value from its disclosure or use, pointing out that this number has been known to chemists since 1909, but not to the general public and certainly cannot be considered a trade secret. Now by amending section 1839, Congress has made clear that the relevant test is whether the information is generally known by "another person who can obtain economic value from the disclosure or use of the information," which is the same standard as under the UTSA.

4. The DTSA Provides for *Ex Parte* Seizures

The DTSA makes the remedy of *ex parte* seizures available to plaintiffs, which allows a plaintiff to seek to have the government seize misappropriated trade secrets without providing advance notice to the defendant. This is perhaps the most controversial provision of the DTSA and there is no comparable provision in any state law. This is potentially an extremely powerful remedy for plaintiffs and is intended to stop the dissemination of a trade secret, especially to overseas, before its value has been lost through public disclosure. Because Congress recognized the potential for abuse of this provision, the DTSA prohibits copies to be made of seized property, and requires the *ex parte* orders to provide specific instruction for law enforcement when the seizure can take place and whether force may used to access locked areas. In addition, a party seeking an *ex parte* seizure must first establish with the court that other less drastic remedies, like a preliminary injunction are inadequate

5. The DTSA Protects Whistle Blowers

The DTSA seeks to protect whistle blowers from criminal or civil liability for disclosing a trade secret if the disclosure is made in confidence to a government official, directly or indirectly, or to an attorney, and it is made for purpose of reporting a violation of law. Employers have an affirmative duty to provide employees notice of the new immunity provision in "any contract or agreement with employee that governs the use of a trade secret or other confidential information." To be in compliance, an employer can, among other things, provide a "cross- reference" to a policy given to the relevant employees that describes the reporting policy for suspected violations of law. Failure to comply means that the employer may not recover exemplary damages or attorney fees in an action brought under the DTSA for theft of trade secrets against an employee to whom no notice was provided. The definition of "employee" is drafted broadly to include contractor and consultant work performed by an individual for an employer.