ALSTON&BIRD

WWW.ALSTON.COM

Intellectual Property / Labor & Employment / Litigation ADVISORY ■

MAY 11, 2016

What the Defend Trade Secrets Act Means for You

Today, President Obama signed the Defend Trade Secrets Act of 2016 (DTSA), which received rare support across party lines, passing Congress unanimously in the Senate and by a vote of 410-2 in the House of Representatives.

Overview

Currently, trade secrets are protected at the state level, and private claims for misappropriation of trade secrets are state law claims. Nearly all states have adopted a version of the Uniform Trade Secrets Act (only New York and Massachusetts protect trade secrets under common law), generally aligning the trade secret definition across states, but important differences between state laws and their application have developed, especially regarding remedies for misappropriation.

Although trade secret theft is already a crime under federal law, the DTSA creates a federal private right of action for misappropriation of trade secrets under the Economic Espionage Act, allowing for the development of a uniform national case law. Similar to trademark protection in the United States, companies will now have the option of seeking redress for trade secret misappropriation in either federal or state court—the bill's drafters expressly provided that the DTSA does not preempt state trade secret laws. A three-year statute of limitations will apply to the federal remedy.

New remedy: Seizure of misappropriated trade secrets in "extraordinary circumstances"

Going farther than states, the DTSA will permit courts to issue orders for the seizure of misappropriated trade secrets—without prior notice to the defendant—to prevent trade secrets from being exploited or shared more widely. After concerns were raised about potential abuses of this new remedy, legislators revised earlier versions of the bill to provide that the seizure remedy would only be available in "extraordinary circumstances." In order for a court to issue a seizure order, the DTSA requires a finding of specific facts by the court showing: (1) "immediate and irreparable injury" would occur absent the seizure; (2) actual possession by the defendant of the trade secret and any property to be seized; (3) a detailed description

of the matter to be seized and the location where it is to be seized; and (4) that the person against whom seizure is sought will "destroy, move, hide, or otherwise make such matter inaccessible to the court, if the applicant were to proceed on notice to such person." As a further deterrent, the DTSA also empowers courts to award damages to defendants for abuses of the seizure remedy by claimants.

Damages for trade secret misappropriation

The new private right of action under the DTSA closely follows the available damages under the Uniform Trade Secrets Act. In claims for misappropriation of trade secrets, the DTSA authorizes courts to award damages totaling the plaintiff's actual loss and any unjust enrichment of the defendant not addressed by the actual losses, or in lieu of those damages, an award of a reasonable royalty. If a trade secret is "willfully and maliciously misappropriated," the DTSA directs that exemplary damages are to be awarded in an amount not to exceed twice the damages or royalty awarded.

What's next?

The new civil cause of action is available immediately in federal courts, but only for trade secret misappropriation taking place after today.

Practical Considerations from the Employment Perspective

Trade secret claims typically arise in the employment context when an employee leaves the company to go work for a competitor and the employee takes or uses the former employer's trade secrets and other confidential information. Trade secret theft can be difficult to prove without actual evidence that the former employee absconded with a physical customer list or sensitive electronic information. Employers typically require, as a condition of employment, that employees agree to additional contractual protections in the form of noncompetition (where and to the extent enforceable), nonsolicitation, nondisclosure and other covenants restricting employee conduct during and after employment.

When a former employee engages in wrongful conduct on behalf of a competitor and the former employer decides to initiate litigation, there are many strategic considerations involved in determining when and where to file a lawsuit and what claims to assert. The DTSA provides an additional claim for employers to consider when evaluating their strategic options, as well as the opportunity to file in federal court. Typically, competition-related disputes between employers and their former employees involve only state law contract and tort claims, and the only path to federal court is through diversity jurisdiction. If the parties are not diverse or the amount in controversy is not yet known or difficult to establish—as can sometimes be the case when a primary goal of the litigation is injunctive relief—filing in federal court is simply not an option. However, the DTSA will open up federal courts when a federal trade secrets claim is asserted, without the requirement of proving diversity and the requisite amount in controversy. This gives employers an additional arrow in their quiver and will undoubtedly be an important strategic consideration in restrictive covenant enforcement cases and litigation over similar types of disputes going forward.

Additionally, two specific provisions in the DTSA may impact cases where employers have asserted federal trade secret claims against competing former employees. First, the Act states that a court cannot issue an injunction preventing a person from entering into an employment relationship, and it further states that

courts can only enter injunctions placing conditions on a person's employment with another company based on evidence of threatened misappropriation and not merely on the information that the person knows. Second, the DTSA provides that a court cannot enter an injunction that conflicts with applicable state law prohibiting restraints on the practice of a lawful profession, trade or business. Companies using the DTSA as an avenue to federal court in an effort to circumvent potentially problematic state law regarding restrictive covenant enforcement and related concerns will have to contend with these important limitations. What effect these provisions will have on lawsuits against former employees involving trade secret claims remains to be seen and will depend significantly on how these provisions are interpreted and applied by the courts.

In addition to new opportunities in litigation, the DTSA also carries with it new obligations for employers—specifically, whistleblower provisions that require employers to modify their nondisclosure agreements going forward or forfeit certain potential remedies under the Act. The DTSA provides a safe harbor for individuals who disclose a trade secret to a government official or attorney for purposes of reporting potential illegal activity. The Act grants both criminal and civil immunity to those individuals under both federal and state trade secret laws. The Act also contains a notice provision requiring employers to notify workers of this immunity in any contract governing the use of trade secrets or other confidential information.

While employers could comply with the notice requirement by adding an express statement to this effect in the agreements themselves, the DTSA also provides that employers can comply with the requirement by including in their agreements a cross-reference to a written policy given to the worker setting forth the employer's reporting policy for suspected illegal activity. Notably, the notice requirement only applies to agreements entered into or modified after the effective date of the DTSA, so employers will not be required to comply with the notice requirement for existing agreements. If an employer does not comply with the notice obligations, it loses the ability to recover exemplary damages or attorneys' fees under the DTSA in any action brought against an employee who did not receive the notice. The Act does not, however, purport to impact an employer's ability to obtain similar remedies under similar state laws protecting trade secrets.

In light of this new obligation that the DTSA places on employers and the impact that it could have both in future trade secrets litigation and in possible investigations by government agencies regarding whistleblower protections for employees, companies should take this opportunity to reexamine their restrictive covenant and nondisclosure agreements, as well as their policies regarding the protection of confidential information and employee whistleblower activities.

Intellectual Property Enforcement Considerations and Impact

Two of the DTSA's sponsors, Senators Orrin Hatch (R-UT) and Chris Coons (D-DE), wrote in a jointly authored Politico op-ed supporting the legislation, "According to some estimates, trade secrets are worth $5 trillion to the U.S. economy, on par with patents. The loss from their misappropriation is substantial—between $160 billion and $480 billion annually."

With these losses in mind, the DTSA could provide a greater incentive for companies to formalize their programs and procedures to identify and protect trade secrets, which would be necessary steps to make effective use of these new enforcement tools. Further, innovators and companies with valuable trade secrets

that are either not eligible or not ideal for patent protection may see greater value in documenting and potentially licensing their trade secret portfolios. Finally, with a uniform federal law and more enforcement teeth, trade secrets may now be recognized with larger valuations in intellectual property portfolios.

Intellectual property enforcement and cybercrime

The DTSA will likely have significant impacts on many aspects of intellectual property litigation, including making federal district courts more of an option for civil enforcement of trade secrets and providing consistency among the numerous jurisdictions where such cases are brought. Because most effective seizure remedies were only available if the Department of Justice chose to investigate and prosecute under federal laws criminalizing the theft of trade secrets, businesses were limited in their ability to prevent harm caused by further exploitation or disclosures. Even when the Department of Justice chose to prosecute trade secret theft, the victimized business had no ability to control when and how that prosecution would take place.

Now, under the DTSA, victims of trade secret theft have this significant civil remedy they have substantially more control over. Congress's passage of the DTSA follows other recent acknowledgments among the international community of the importance of protecting trade secrets, including the inclusion of trade secrets provisions in the Trans-Pacific Partnership agreement, the amendments taking effect earlier this year to Japan's Unfair Competition Prevention Act and the adoption of the Trade Secrets Directive by the European Parliament earlier this month.

The DTSA can also provide a helpful tool for victims of cybercrime and espionage. The new private cause of action empowers corporate victims of cyber-enabled trade secret theft or espionage to recover from perpetrators, again making victims less dependent on government criminal action. If jurisdiction can be obtained over the perpetrators (or over the misappropriated trade secret property), the new seizure remedy would enable victims of corporate theft to recover stolen information and data before it can be disclosed, and the damages awards made available by the DTSA would allow victims to recover resulting losses.

Impact of DTSA on IP decision-making

The DTSA will likely impact patent counseling and prosecution practice and decisions by companies and inventors involving whether to seek patent protection or attempt to protect inventions as trade secrets, particularly if trade secret protection becomes more consistent and predictable as a result of the DTSA. Unlike patent protection, which is only available for a fixed term, a trade secret can be maintained for as long as the information is successfully kept secret. Of course, in many instances trade secret protection is unavailable for information that is disclosed or involves products capable of being copied or reverse engineered. However, many industries do rely on trade secret laws to protect their most valuable, intangible assets.

A common misconception is that trade secret protection is only available to limited industry sectors. Traditionally, information such as manufacturing processes or products with "secret ingredients" that were difficult to reverse engineer were viewed as more typical candidates for trade secret protection, along with customer lists, financial metrics and marketing plans. But advances in technology have made it possible to transmit data and information rapidly, enabling companies to maintain a broader range of technology as trade secrets by limiting the extent to which disclosures are required in order to provide certain services.

For example, although software may have been historically difficult to protect as a trade secret, the DTSA received substantial support from software lobbyists representing Apple and Microsoft. This is unsurprising given that cloud computing, software as a service and data processing have enabled software and algorithms to be protected in back-office operations as a trade secret. Trade secret protection is well suited for a wider range of processes and methods that are not disclosed by putting products or services out in the stream of commerce.

Several recent Supreme Court decisions widely viewed to limit the availability of patent protection (e.g., *Mayo v. Prometheus, Association for Molecular Pathology v. Myriad Genetics* and *Alice Corp. v. CLS Bank International*) will likely further bolster the appeal of protecting certain technology as trade secrets, where feasible. Even before these cases were decided, in some industries companies had already found more practical reasons for keeping their innovations as trade secrets in lieu of seeking patent protection. In a 2012 interview with *Wired* magazine, entrepreneur Elon Musk explained, "We have essentially no patents in SpaceX." Explaining that seeking patent protection in some circumstances is akin to publishing a "recipe book," Musk can only mean that he fully intends to protect SpaceX's many methods, designs, tools, etc., as trade secrets. With the passage of the DTSA, SpaceX and companies employing a similar strategy will potentially have a new enforcement tool with significant teeth.

Minimum Requirements to Access the DTSA's Remedies and Other Benefits

Of course, none of these remedies or considerations are available to a company that does not take certain steps to document and protect its trade secrets. The DTSA's passage is a good time for businesses to consider some basic questions about trade secrets that may be valuable parts of their IP portfolios:

- Do you have a good sense of what your trade secrets are?
- What programs and procedures does your company use to identify and document trade secrets?
- Who has access to your company's trade secrets, and on what basis is that access limited?
- Have you considered whether more value could be realized from patent-eligible inventions by instead protecting them as trade secrets under the DTSA and, if so, what criteria do you use?
- Does your company require all employees and contractors to sign confidentiality or nondisclosure agreements to protect trade secrets?
- Has your company developed a plan to update confidentiality and nondisclosure agreements to comply with the DTSA (e.g., whistleblower protections)?

Final Thoughts

The DTSA has implications for most businesses for their employment practices and the management, protection and enforcement of their intellectual property. Making an early assessment of how best to respond to the new law (and updating relevant documents) and considering trade secret protection as an alternative to patents will be prudent at least and potentially value enhancing.

If you would like to receive future ***Intellectual Property*** advisories electronically, please forward your contact information to **ip.advisory@alston.com**. If you would like to receive future ***Labor & Employment*** advisories electronically, please forward your contact information to **labor.advisory@alston.com**. Be sure to put "**subscribe**" in the subject line.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or any attorney listed below.

Intellectual Property

Keith Broyles
404.881.7558
keith.broyles@alston.com

Jason Cooper
404.881.4831
jason.cooper@alston.com

Brian Ellsworth
704.444.1265
brian.ellsworth@alston.com

Guy Gosnell
704.444.1029
guy.gosnell@alston.com

Jonathan Gordon
213.576.1165
jonathan.gordon@alston.com

Michael Newton
214.922.3423
mike.newton@alston.com

Bruce Rose
704.444.1036
bruce.rose@alston.com

David Teske
4040.881.7935
david.teske@alston.com

Jesse Welsh-Keyser
213.576.1188
jesse.welsh-keyser@alston.com

Privacy & Data Security

James Harvey
404.881.7328
jim.harvey@alston.com

Kimberly Peretti
202.239.3720
kimberly.peretti@alston.com

Michael Zweiback
213.576.1186
michael.zweiback@alston.com

Labor & Employment

Lisa Cassilly
404.881.7945
lisa.cassilly@alston.com

Brett Coburn
404.881.4990
brett.coburn@alston.com

Christopher Marquardt
404.881.7827
chris.marquardt@alston.com

Kristen Fox
404.881.4284
kristen.fox@alston.com

Litigation

James Grant
404.881.7859
jim.grant@alston.com

Daniel Norris
404.881.7826
daniel.norris@alston.com

Edward Bonapfel
404.881.7166
ed.bonapfel@alston.com

ALSTON&BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: 2828 North Harwood Street ■ 18th Floor ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RESEARCH TRIANGLE: 4721 Emperor Blvd. ■ Suite 400 ■ Durham, North Carolina, USA, 27703-85802 ■ 919.862.2200 ■ Fax: 919.862.2260
SILICON VALLEY: 1950 University Avenue ■ 5th Floor ■ East Palo Alto, California, USA, 94303-2282 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333