REPRINT

CD corporate disputes

IMPACT OF THE DEFEND TRADE SECRETS ACT IN THE US

REPRINTED FROM:
CORPORATE DISPUTES MAGAZINE
JAN-MAR 2017 ISSUE

www.corporatedisputesmagazine.com

Visit the website to request
a free copy of the full e-magazine

manatt

Published by Financier Worldwide Ltd
corporatedisputes@financierworldwide.com

MINI-ROUNDTABLE

IMPACT OF THE DEFEND TRADE SECRETS ACT IN THE US

PANEL EXPERTS

Michelle A. Cooke
Partner
Manatt, Phelps & Phillips, LLP
T: +1 (310) 312 4208
E: mcooke@manatt.com

Michelle Cooke helps intellectual property owners build, protect and monetise their assets globally, including in the digital marketplace. Focusing on brand usage, management and development, and online content, she provides and handles risk assessments, counselling, licensing, acquisitions and sales, international protection and enforcement strategies and tactical portfolio building in connection with intellectual property assets. She also has particular experience with the entertainment and media, multimedia platforms, consumer products, apparel, software industries and online service providers.

Rebecca L. Torrey
Partner
Manatt, Phelps & Phillips, LLP
T: +1 (310) 312 4172
E: rtorrey@manatt.com

Rebecca Torrey is experienced in all aspects of employment law, with an emphasis on defending employers in bet the company cases in federal and state courts. She regularly advises organisations in the full range of employment matters, including trade secrets protections and the use of nondisclosure agreements and non-competition agreements, and compliance with state and federal laws. Her clients range from Fortune 50 companies and middle market companies, to start-ups in a wide range of industries.

CD: Could you provide some insight into how the Defend Trade Secrets Act (DTSA) has been received since it was signed into law in May 2016? How does it compare with the protection afforded by the Uniform Trade Secrets Act (UTSA) adopted by most states (New York and Massachusetts aside)?

Cooke: The DTSA largely has been welcomed by business communities. It is anticipated that the DTSA will be a significant tool to better protect some of the most valuable business assets of the modern economy – information. This is particularly important given the ease and speed by which complex and voluminous information can be copied and distributed globally. Previously, many businesses found existing legal remedies insufficient to protect their trade secrets in the event of a violation. As with any new major law, the DTSA's shortcomings may not come to light fully for several years. However, yellow flags have already been raised by some on whether the injunction and seizure remedies might tilt too much in favour of the alleged victim, and whether the DTSA favours larger entities to the detriment of smaller businesses and individual employees.

Torrey: The DTSA passed both houses of Congress with overwhelming support and has received widespread attention in business and legal commentary following its enactment. It is the first federal law in the US to create a civil cause of action for trade secret theft, allowing litigants access to federal courts and providing a statute nationwide to protect trade secrets uniformly. It amends the Economic Espionage Act, which provides criminal prosecution for trade secret theft. The DTSA defines trade secrets in a similar fashion to the UTSA state laws and offers some of the same remedies. In addition to financial damages and injunctive relief commonly available under the pre-existing patchwork of state laws, the DTSA provides a unique seizure remedy, empowering the court on an ex parte basis to seize data or products embodying trade secrets, pending the outcome of the litigation. One strategic advantage it offers is the easy enforcement of a federal preliminary or permanent court order nationwide, without the need for time consuming and costly ancillary legal action, outside of the state where a lawsuit is initiated.

CD: How do you foresee the DTSA working in tandem with extant state trade secret laws? What safeguards are in place to help ensure that the new federal law supplements, rather than pre-empts, state laws?

Torrey: The DTSA expressly does not pre-empt state trade secrets laws; rather; it provides additional

remedies and strategic options that are likely to impact the outcome of a claim. Litigants may simultaneously allege claims under both federal and state trade secrets laws and select a state or federal forum to litigate those claims. One could even litigate separate actions in state and federal courts if there was an advantage in doing so. Some state laws provide defences and remedies that the DTSA does not, for example, the California requirement to identify trade secrets with particularity to maintain an action is not part of the DTSA. Other state laws accept legal theories rejected by the DTSA, for instance, the inevitable disclosure doctrine. A business concerned about misappropriation should strategically evaluate what benefits the DTSA and state laws offer, and utilise a deep understanding of all options in initiating or defending trade secret actions.

Cooke: Any major new law creates the possibility of increased litigation. The hope for the DTSA is that it will, in part, fill a gap in the protection of intellectual property rights. With the additional remedies available within the DTSA, owners may now be more willing to go to court than previously. Until the courts have time to build precedent interpreting and applying the DTSA, even the potential for additional relief might encourage more suits. Increased litigation arising under the DTSA raises the legitimate worry of the impact of the DTSA on the US' already clogged federal court system. The seizure provisions of the DTSA, with required expedited handling, will further add to the courts' workload. However, from the perspective of trade secret owners, particularly those with multi-state operations, the availability of a uniform federal legal scheme might provide increased efficiency in the handling of trade secret misappropriations, with potentially more consistent results across the US.

CD: Could you outline the wider provision the DTSA makes for technology-related concerns, such as mobile devices, privacy and cyber breach issues? As regards the 'ex parte seizure' provision of the DTSA, what particular threshold does an affidavit or verified complaint need to reach so that an ex parte order can be obtained?

Cooke: Targets of cyber crime expect the DTSA to provide them with additional and critical support when trying to stop, or at least limit, the exposure of trade secrets stolen through electronic data breaches. In particular, unlike state trade secret laws, the DTSA promises to be quicker and more nimble in stopping stolen trade secrets from leaving the country. Given the broad extent of data breaches, some of which use technology to mask that the breach even occurred or the length of the breach, the DTSA should provide additional remedies for the growing class of cyber crime victims.

Torrey: In our digital age, trade secrets theft is effectuated primarily by external hacking or by employees. Theft of data has become easier to accomplish and more expensive to trace as businesses rely heavily on electronic storage and transmission of information. The ex parte seizure process is suited to address the theft of trade secrets embodied in digital data, whether on mobile devices or otherwise. Litigants seeking judicial seizure must show that provisional remedies, including injunctions, are inadequate and that extraordinary circumstances exist to justify immediate seizure. Applicants must offer factual proof of the likelihood of success that the information is a trade secret, the person involved in misappropriation used or conspired to use improper means to obtain it, that he or she has actual possession of trade secrets and where those trade secrets are physically located, among other things. For ex parte relief, the applicant must show that the person in possession would destroy, move, hide or make the data inaccessible to the court if advance notice of the seizure was provided. While the seizure mechanism is a powerful new tool, there is little guidance outside the statute on how the seizure process will work in practice because, to date, the process is largely untried.

CD: With IP protection becoming a key consideration in today's highly competitive business world, how important is it for companies to train their employees to abide by trade secret laws so that they can recognise trade secrets and other confidential information, and mitigate the risk of its loss or theft?

> **"Companies tend to take one of two routes regarding their trade secrets. The first route is to invest very little in their protection. The second route is the kitchen-sink approach."**
>
> *Michelle A. Cooke, Manatt, Phelps & Phillips, LLP*

Torrey: Most companies neglect the basic steps required to protect against accidental or intentional disclosures. Efforts are typically limited to out-of-date non-disclosure forms signed by employees at the time of hire. In addition to signing a well-crafted non-disclosure agreement (NDA) that each employee clearly understands, employees must be taught what specific information, processes or products

in the workplace are regarded as trade secrets, what steps they individually must take on a daily basis to maintain them in confidence, how to avoid inadvertent disclosures and what to do immediately in the event of a breach. Employees need to have a thorough understanding of how to detect data security threats from outsiders. Deliberate, insightful and repeated training is crucial. Companies that limit the responsibility for trade secret protections to human resources or legal are not adequately protecting their assets.

Cooke: Companies tend to take one of two routes regarding their trade secrets. The first route is to invest very little in their protection. When there has been a perceived theft, perhaps by a key employee that joins a competitor, these companies then may try to assert a claim for misappropriation. In these instances, the information at issue may not even qualify as a trade secret because the company failed to implement appropriate internal protection mechanisms and procedures. The second route is the kitchen-sink approach. The company adopts a policy that everything the employee is exposed to at work is a company trade secret which, if vague and overly-broad, can create enforceability problems. Companies must take the time to identify what information, data and methods they have that qualify as trade secrets. Once the trade secrets have been identified, existing protection measures should be revisited to help ensure that trade secret status can be maintained. For valuable data that is developed in the future, the company should already have in place procedures and protocols to ensure that assets are identified in a timely fashion and are properly protected as trade secrets.

CD: How would you characterise the scope and application of the whistleblower protection/immunity provisions included in the DTSA? Should companies review their general policies and procedures pertaining to their trade secrets, in light of the new federal protection?

Cooke: This provision prevents employers from turning the DTSA into a weapon to discourage whistleblowing. As such, there are a number of penalties that an employer could face for failing to notify employees of the immunity that applies to whistleblowers. Employers concerned that employees might try to avail themselves of this immunity provision if they disseminate trade secrets broadly can take a measure of comfort that this provision only applies to the disclosure of a trade secret in confidence to either the government or an attorney, and for the sole purpose of reporting or investigating a potential legal violation. The immunity provision also applies to trade secrets disclosed in a lawsuit or other legal proceeding, provided that the disclosures were made under seal.

Torrey: The whistleblower protection and immunity provisions are a key element of the DTSA and an important development in the law. Businesses seeking to protect trade secrets must expressly notify employees that nothing prohibits them from freely communicating and reporting, in good faith, any violations of law or regulation or from providing confidential information learned in employment to any government authority, among other detailed notice requirements. Employees who report confidential information in good faith are immune from civil liability and legally protected from retaliation in employment. Failure to comply with this statutory obligation can significantly limit protections a company may have under DTSA and lead to serious problems with various federal agencies including the Securities and Exchange Commission.

CD: What advice can you offer to companies on utilising the DTSA to protect their IP interests? How should they interpret the new statute in the context of their litigation options?

Torrey: Companies must update and have employees re-sign all pre-May 2016 NDAs, employment and contractor agreements and confidentiality policies, and implement training programmes to track the requirements of the DTSA. The need for up-to-date agreements is critical because certain DTSA remedies, such as exemplary damages, are unavailable if employees are not advised in advance of specific whistleblower protections. Management should put protocols in place to counsel new employees at the time of hire about internal trade secret protections and the risks of using trade secrets from a prior employer, refreshing these protocols by training personnel regularly during the course of employment. Organisations need to be proactive and take intelligent steps to prevent trade secret theft, principally by creating a healthy culture of loyalty to the company among employees, in addition to implementing preventive measures and monitoring for breaches. Preparation includes being adept at responding to DTSA claims effectively, because trade secret litigation often moves rapidly with very short response times. A good defence can avert potentially restrictive and expensive consequences for business going forward.

Cooke: Many companies have proprietary and confidential information which potentially could meet the standard of a trade secret – does the information derive independent economic value from not being generally known to, and not readily ascertainable through proper means, by another who could obtain economic value from the disclosure or use of that information? However, if the owner fails to take reasonable steps to keep the foregoing information secret, then it is not protectable as a trade secret. The implementation of

the DTSA is an ideal opportunity – if not a wake-up call – for business and intellectual property owners to create an honest inventory of their trade secrets. Next, the policies, procedures and documents – including employee acknowledgement forms – should be reviewed and revised to meet the standards of the DTSA, as well as applicable state trade secret laws. In addition to conducting an inward review, companies also need to examine their defences to outside attack, specifically, security measures and protocols as to the access and utilisation of their data and electronic files. Cyber security is essential to every business. As a result, companies, at a bare minimum, need to take reasonable measures to ensure that their cyber security equipment, protocols, training and methods are up-to-date and appropriate for the type of data at issue.

CD: What do you consider to be the likely impact of the DTSA on the trade secret strategies adopted by companies in the future?

Torrey: With the attention to trade secret theft that the DTSA has brought, companies should be more attuned to identifying and taking steps to protect their intellectual property and proprietary information. We have already seen organisations focus on added protections and training and we expect that trend to continue. Every business has something critically valuable to protect.

> **"A good defence can avert potentially restrictive and expensive consequences for business going forward."**
>
> *Rebecca L. Torrey, Manatt, Phelps & Phillips, LLP*

Cooke: This is a key point – protecting the corporate value of intellectual property. This may require employing different strategies for different types of intellectual property. Unlike patents or trademarks, for example, there is no trade secrets registrar. This places solely on the company the continuous burden of ensuring that its trade secrets are properly used and protected from unnecessary and unauthorised access by its own employees, consultants and agents, as well as shielded against external exposure. Failure to take these steps puts valuable information at risk. As the DTSA is providing additional remedies to help protect trade secrets, we anticipate that more companies may

implement procedures to try to qualify trade secret status for business critical information.

CD: How do you see the new statute developing and evolving in the months and years to come? Are we likely to see a radical uptick in the number of trade secret claims pursued in the US?

Torrey: As cases are filed across the country, judicial interpretation of the statute will fill gaps in our understanding of the DTSA and its practical application. We anticipate regional and industry trends with potential splits in the federal circuits which may eventually work their way up to the Supreme Court. Although we expect an uptick in trade secret claims, it will mainly occur because of the relatively easy access to digital information and rise in data security breaches, not necessarily due to the enactment of the DTSA.

Cooke: I agree that more litigation will arise under the DTSA due to the growing pervasiveness of cyber theft. However, because the DTSA in theory can apply to all trade secrets – not just data breaches—and is offering remedies and ready access to federal courts that may not have been previously available, I anticipate that there generally will be an increase in trade secret claims – at least until the courts have an opportunity to develop case law on the DTSA, which will provide potential plaintiffs and defendants more detailed guidance in evaluating the merits of their positions in determining whether a lawsuit is the best route for them. CD