Published on *The National Law Review* https://natlawreview.com

COVID-19 Update: Protecting Trade Secrets In The Midst Of The COVID-19 Pandemic

Article By:

John T. Moehringer

Danielle Vincenti Tully

Michael B. Powell

Millions of Americans and others around the globe have been told to work from home in order to blunt the spread of COVID-19. In short order, companies have been faced with unprecedented strain on internal networks and demands from employees to access confidential business information from home. While the COVID-19 Pandemic presents serious challenges to public health and the economy, the extraordinary access of confidential business information at home should present a lurking concern for companies, since employees themselves are typically the largest source of trade secret misappropriation. Moreover, cybercriminals may prey on employees inexperienced with working from home and those who fail to follow proper cyber-hygiene.

During this new era of forced remote working—at levels unthinkable mere months ago—sensitive technical information, business know-how, customer lists, and even HR records are being routed to employee's homes, where they might be copied and disseminated in an unsecured manner. Further, employees are turning to Zoom and Webex meetings at unequaled levels during the Pandemic to host meetings. The increased level of such interactive videoconferencing software represents a new risk where third parties, that are not under obligations of confidentiality, may be included and exposed to trade secrets even if inadvertently. This new age of home offices may also lead to a higher level of job mobility, which will only increase the risk that employees who had access to important trade secrets may be working for a competitor in the future.

The Defend Trade Secrets Act ("DTSA") provides a way for companies to mitigate the damage caused by the unauthorized dissemination of confidential business information. The DTSA provides a federal cause of action allowing for injunctive relief, money damages, and in extraordinary circumstances, *ex parte* seizure of property when "necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action."[1] The DTSA broadly defines trade secrets as "all forms and types of financial, business, scientific, technical, economic, or engineering information[.]"[2] The term "misappropriation" is defined to include the acquisition, disclosure or use of a trade secret.[3]

The DTSA amended and supplemented sections of the previously enacted Economic Espionage Act of 1996, but left unchanged the explicit application of the statute to conduct occurring outside the United States when:

1. the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or

2. an act in furtherance of the offense was committed in the United States.[4]

A number of district courts have held that the private cause of action created by § 1836 is likewise extraterritorial.[5] In particular, two recent decisions highlight the capability to use the DTSA to protect against misappropriation of trade secrets through remote access by employees or third parties—even beyond the borders of the United States.

In *Motorola*, three engineers were hired away by another firm abroad, and those engineers stole and brought trade secrets with them to their new employer.[6] The Northern District of Illinois allowed for extraterritorial damages—*i.e.*, damages relating to conduct occurring outside the United States—because evidence existed that the defendant had "used" the alleged trade secret in the United States, including by marketing products in the United States embodying the alleged trade secrets.[7]

Similarly, in *vPersonalize*, a United Kingdom-based defendant acquired trade secrets that had been downloaded by a third party in the United States. In rejecting the defendant's motion to dismiss, the Western District of Washington held that foreign entities were subject to the DTSA and, further, reasoned that the "in furtherance of the offense" requirement of § 1837(2) could be met vicariously via the domestic acts of a third party or directly via the defendant's attempts to market products and services embodying the trade secrets within the United States.[8]

Given the global reach of both many corporations and the COVID-19 Pandemic, such interpretations provide increased assurances to corporations that they can redress the harms caused by trade secret misappropriations—wherever they might occur.[9]

Recommendations

It is more important than ever before that companies maintain reasonable measures to safeguard confidential business information. Companies should ensure that access to sensitive information is only given to those employees who truly require access to further company business objectives.

In addition to using industry best practices to maintain such information on company systems, companies should remind remote employees to maintain proper cyber-hygiene, and to avoid any unnecessary dissemination of company information.

U.S.-based legal departments should also consider providing a notice to remote employees, including those that are only temporarily working remotely because of the COVID-19 pandemic, before being given access to confidential systems, that expressly acknowledges the sensitive nature of the company's confidential business information, encourages the employee to practice proper cyber-hygiene, and affirms that the employee will not engage in unauthorized dissemination of company trade secrets.

This will remind all employees who may find themselves working remotely to maintain the integrity of confidential business information, and in the event a misappropriation of trade secret occurs, provide evidence that can be used to prove a violation and, potentially, that an act in furtherance of the offense occurred in the United States.

In addition, any employee that is leaving the company should be asked to sign a certification acknowledging that they were aware of the obligation to maintain firm trade secrets, that they have complied and that they understand any future violation would be subject to action under the DTSA.

Finally, companies should be ready to act quickly, including possibly pursuing a seizure remedy, if they believe a trade secret has been jeopardized in some way by an employee or a cybercriminal.

---

1 18 U.S.C § 1836.

2 18 U.S.C § 1839(3).

3 18 U.S.C § 1839 (5).

4 18 U.S.C § 1837.

5 *See Motorola Solutions Inc., v. Hytera Comm. Corp.*, 1:17-cv-1973, ECF No. 834 at 1, 25 (N.D. Ill., Jan. 31, 2020); *vPersonalize Inc. v. Magnetize Consultants Ltd.*, No. 2:18-CV-01836-BJR, 2020 WL 534505, at *12-13 (W.D. Wash., Feb. 3, 2020); *see also Motorola*, 1:17-cv-1973, ECF No. 834 at 10-11 (listing District Court decisions finding extraterritorial application and noting that it did not identify any court that has held the DTSA does not apply extraterritorially to private rights of action).

6 *Motorola*, 1:17-cv-1973, ECF No. 834 at 1-2.

7 *Id.* at 21.

8 *vPersonalize*, No. 2:18-CV-01836-BJR, 2020 WL 534505, at *12-13.

9 Additionally, unlike actions for patent infringement, DTSA causes of action are subject to the general venue provisions of 28 U.S.C. § 1391, meaning that venue is proper in any district court where personal jurisdiction exists.

National Law Review, Volume X, Number 92