Articles + Publications | August 13, 2020

Protecting Trade Secrets: Lessons Learned From the Levandowski Case

WRITTEN BY

Gwendolyn Tawresey | Miranda Hooker

RELATED OFFICES

Boston

Companies often consider trade secrets to be their crown jewels. But in the digital age, where copying and sending files is as easy as one click, protecting trade secrets has become even more challenging. Losing control over a trade secret can mean losing the edge over competitors or possibly the entire value of a product or a company. This article discusses recent developments in trade secret law, including the prosecution and sentencing of Anthony Levandowski, who pleaded guilty to one count of trade secret theft under 18 U.S.C. § 1832(a)(1) and was sentenced to 18 months in prison. We also compare the contours of this criminal proceeding with a civil action related to the same theft. While the Levandowski case is evidence that the Department of Justice has become more active in trade secret prosecutions, companies still must be proactive in monitoring cyber activities to protect their valuable trade secrets.

Background

In 1996, the United States enacted the Economic Espionage Act (EEA), which made trade secret theft a federal crime. Before the EEA, the United States left governance of trade secrets to the states. The EEA provided, for the first time, a federal definition of “trade secrets” that includes all forms and types of information that the owner took reasonable steps to keep secret, and that derives independent economic value from not being generally known to or ascertainable through proper means by another who can obtain economic value from the information. In 2016, Congress amended the EEA with the Defend Trade Secrets Act (DTSA), which created a private federal cause of action for trade secret theft and allowed companies to obtain either an injunction, preventing further use of the trade secret, or monetary damages. Although the DTSA created civil remedies under federal law, it did not supplant state law, leaving criminal prosecution under the EEA and civil actions under both the DTSA and state law available to remedy trade secret theft.

Levandowski Case

All three types of action were pursued in the Levandowski case. In December 2015, Levandowski, a former manager at self-driving technology company Waymo, left the company and allegedly downloaded more than 14,000 confidential and proprietary documents before doing so. Levandowski then started his own self-driving technology companies, Ottomoto, LLC and Otto Trucking, LLC (collectively, Otto). Uber purchased Otto in August 2016 for $680 million. In February 2017, Waymo filed a civil complaint raising DTSA and state law violations and

alleging that Uber and Otto relied on the documents Levandowski stole to develop imaging technology for their self-driving cars, rather than developing it independently. Five days into the jury trial, the parties entered into a settlement agreement, pursuant to which Uber agreed not to use any of Waymo's technology in its self-driving cars and to give Waymo 0.34% of its equity, equivalent to $245 million.

In August 2019, a grand jury in San Jose indicted Levandowski on criminal charges of trade secret theft under the EEA, 18 U.S.C. § 1832. The indictment charged Levandowski with 33 counts, with each count corresponding to a different document allegedly taken by Levandowski. In March 2020, Levandowski pleaded guilty to one count of trade secret theft, corresponding to a single "weekly updates" document. While Levandowski admitted to downloading and taking 20 documents, the "weekly updates" document is the only one he admitted to downloading "with the intent to use it for the benefit of someone other than [Waymo]." For the purpose of determining his sentence, Levandowski agreed to value the "weekly updates" document between $550,000 and $1.5 million, bringing his recommended sentence as a first-time offender to between 24 and 30 months. Ultimately, Judge William Alsup sentenced Levandowski to 18 months in prison, followed by three years of supervised release; a $95,000 fine; and payment of $756,499.22 in restitution to Waymo. Judge Alsup commented at the sentencing hearing that Levandowski committed "the biggest trade secret crime I have ever seen" and that a noncustodial sentence would be a "a green light to every future brilliant engineer to steal trade secrets." Levandowski declared bankruptcy in March 2020, but restitution included in a criminal sentencing cannot be discharged through any type of bankruptcy proceeding.

Takeaways

The Levandowski disputes highlight important lessons for companies seeking to ensure that their trade secrets are adequately protected and, if anything happens, that they will be protected under the relevant laws.

- **Require employees to sign nondisclosure agreements (NDAs)**. The initial, and most critical, step a company should take to protect trade secrets is to create an NDA and require employees to sign it. NDAs are legally binding documents that put employees on notice that they are not permitted to share a company's confidential information at any time, including after the employment relationship is terminated.

- **Identify your company's trade secrets early and often**. Every company with trade secrets should have a written policy to tell employees how to identify and protect trade secrets. This assists employees in understanding what belongs to the company and prevents inadvertent trade secret disclosure.

- **Take adequate steps to protect confidential information**. In addition to making clear to employees what information is considered a trade secret, companies should take steps to ensure that access to this information is appropriately restricted and protected. For example, store documents reflecting trade secrets in locked cabinets, or house electronic documents in secured data rooms that are password-protected and restricted to only those employees who require access.

- **Companies should inform their employees that using and copying documents is monitored — and then monitor that activity.** In the Levandowski case, forensic analysis of electronic devices formed a key aspect of the proof that Levandowski had taken confidential documents with him when he left Waymo. Tracking the use and copying of documents internally can help prove trade secret theft when it happens, and informing employees that document use is being monitored can also deter theft.

- **If trade secrets are stolen, consider pursuing both civil and criminal remedies.** Levandowski's theft of Waymo's trade secrets resulted in both criminal penalties for Levandowski and a civil settlement against Uber.

The criminal penalty against Levandowski benefits Waymo by showing its current employees how seriously it takes its trade secrets, potentially having a deterrent effect on future trade secret theft. The civil case likewise benefitted Waymo by giving it an ownership stake in one of its biggest competitors. While the trade secret disclosure cannot be undone, this civil remedy may undo some of the competitive damage Levandowski caused to Waymo by giving its secrets to Uber. The ownership stake also gives Waymo some insight into Uber's operations, allowing easier enforcement of the non-use provision of the settlement.

RELATED INDUSTRIES + PRACTICES

- Intellectual Property
- White Collar Litigation + Investigations