SEBRIS BUSTO JAMES Employment Law Note April 2017

The Defend Trade Secrets Act
(and Other Ways to Protect your Company's Confidential Information)
By Jason Rossiter

Waymo is the self-driving car subsidiary of Google's parent Alphabet Inc. On February 23, 2017, Waymo filed a lawsuit in federal court in San Francisco, accusing Uber and two other companies of stealing its trade secrets. The allegations in the lawsuit are unproven—but offer important lessons to businesses who are eager to protect their trade secrets from theft.

Waymo's lawsuit is focused on the alleged actions of the former head of Waymo's self-driving car project, Anthony Levandowski. Mr. Levandowski left Waymo in January of 2016 to found a company called Otto, which sells kits that give self-driving capabilities to semi-trailer trucks. Uber acquired Otto just eight months later. In its lawsuit, Waymo makes some stunning allegations:

> In December 2015, Mr. Levandowski specifically searched for and then installed specialized software onto his company-issued laptop in order to access the server… . Once Mr. Levandowski accessed this server, he downloaded the 14,000 files, representing approximately 9.7 GB of highly confidential data. Then he attached an external drive to the laptop for a period of eight hours. He installed a new operating system that would have the effect of reformatting his laptop, attempting to erase any forensic fingerprints that would show what he did with Waymo's valuable LiDAR designs once they had been downloaded to his computer. After Mr. Levandowski wiped this laptop, he only used it for a few minutes, and then inexplicably never used it again.

Waymo claims to have discovered the theft after being copied on an email by a vendor containing "drawings of what purports to be an Uber LiDAR circuit board" that bore "a striking resemblance" to Waymo's own design.

Mr. Levandowski, Otto, and Uber may not have done what they are accused of doing. Yet there are important lessons for employers in the allegations themselves.

Watchfulness is Critical, Because Prevention Only Goes So Far

There are many protective measures that organizations implement to prevent employee data theft and unauthorized network access: firewalls, anti-malware software, network segmentation, hardware restrictions, etc. And Waymo appears to have done some of these things: its Complaint notes that the trade secrets were located on a separate server that required "specialized software." This was evidently not enough to stop this theft. Waymo's lawsuit is an important reminder that if an employee is determined or resourceful enough, they will get in and steal your data. Your employees may be more technologically sophisticated than your IT staff. This makes *monitoring* just as critical as prevention, if not more so. The sooner you detect that your barn door is open, the more likely that you will be able to recover your horses.

Even by Waymo's telling of its story, there are things that it might have spotted sooner. 9.7 GB is a *lot* of data, more than many employees would ordinarily have a legitimate need to move across a network. Perhaps nobody noticed this much data leaving the server, or crossing the network, or that it was all headed to a single location. It can be expensive and annoying for an organization to pay an army of IT employees to benchmark its network and server traffic so that the company knows what "normal" looks like, or to pore over logs to check for unusual activity. But even if 9.7 GB files were "normal" at Waymo, *in this particular case* it wasn't normal at all. Had someone been reviewing the right logs, it might have been possible to flag this theft sooner.

When You Spot Trouble, Act Quickly

One thing Waymo evidently got right was that as soon as it discovered that something was amiss, it acted quickly. Part of the reason that Waymo was able to learn so much about how this particular theft occurred

was because (for example) the laptop in question had apparently not yet been wiped and handed off to some other employee.

When a company needs to go to court to protect its trade secrets, timing is critical. Frequently, once technical or customer data is in the hands—or the minds—of the wrong person, there is little that can be done to undo the damage. But if too much time has passed, evidence that the company may need to prove the theft can also vanish. Computers get reassigned. Logs get overwritten. Quick action is essential once wrongdoing is suspected to make sure that proof of the theft remains possible. And once the theft is discovered, courts will sometimes find that a company has waived its rights if it waits too long before going to court. It can be inconsistent for a company to claim that its very existence is threatened by a potential loss of trade secrets if that same company delayed bringing the lawsuit. Maybe there are legitimate reasons for a delay, but a company who is sitting on a possible lawsuit, but who has not brought it, had better be prepared to explain what is taking so long.

Update Your Nondisclosure Agreements

Notice that Waymo was able to file its lawsuit in *federal* court, rather than in state court. One reason that it may have had this option was because of a new law that was passed in 2016 called the Defend Trade Secrets Act. Before the Defend Trade Secrets Act, the only way to sue in federal court for a trade secret theft was if the parties were "citizens" of different states and enough money was in controversy (unless some other federal law happened to have been violated as well).

But the Defend Trade Secrets Act makes it possible to sue in federal court, so long as the trade secrets in question were meant for use in interstate commerce. This new law gives federal courts the power not only to award damages, but to award royalties, issue injunctions and seizure orders against trade secret thieves, and award theft victims "exemplary" damages (essentially, double damages) and attorneys' fees.

However, this law also requires that employers must include a disclosure in any new nondisclosure agreements or similar contracts that the employer enters into with its employees. This disclosure informs the employee of his or her rights to make limited disclosures of trade secrets in the course of initiating whistleblowing proceedings. The penalty for employers who fail to include this disclosure in new agreements is that the employer loses the right to recover either "exemplary" damages or attorneys' fees in any Defend Trade Secrets Act claim.

This is a potentially serious consequence, because the prospect of having to potentially pay exemplary damages as well as the enforcing employer's attorneys' fees is often a key factor in dissuading trade secret theft in the first place. Employers should ensure that their employee nondisclosure agreements, noncompete agreements, and similar contracts are updated to include this new disclosure language.