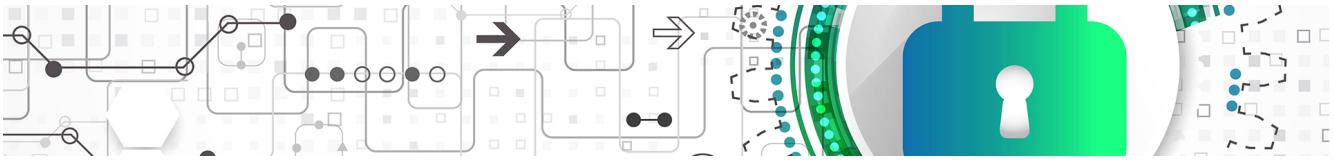

Uber / Google Trade Secret Row Over Self-Driving Car Tech Hits End of Road: Settlement and Jail Time

August 6, 2020

By Noel Courage

It appears that the key civil and criminal aspects of this fascinating case about trade secret intellectual property are now complete, after a former employee was recently sentenced in criminal court for trade secret theft. A recap, and some lessons learned about trade secrets, are provided in this article.

The legal battle began in 2017 after Waymo, a Google spin-off, received an inadvertent email from a supplier about light detection technology called "**LiDAR**." The email contained drawings of what appeared to be Uber's LiDAR circuit board, except the design looked a lot like Waymo's LiDAR design. Waymo then determined that a former employee downloaded, 6 weeks before leaving, over 14,000 design files (9.7GB) including circuit boards and other light detection technology. The former employee had left Waymo to go work for a startup called Otto, which was acquired by Uber. Waymo started a court action against Uber, alleging trade secret misappropriation, patent infringement and unfair competition. The lawsuit requested damages and an injunction against Uber. The companies settled the lawsuit in 2018 in the midst of their high-stakes trial. Uber cried uncle under the looming threat of liability and an injunction, agreeing to pay Waymo a settlement of 0.34% of Uber equity (worth about US$245m at that time). Uber also expressed regret and agreed to ensure that Waymo confidential information was not incorporated into Uber technology.

The former employee was fired by Uber in May 2017. He was also criminally charged for the trade secret theft, and reached a plea bargain in return for a guilty plea (a number of other charges were dropped). In August 2020, he was sentenced to 18 months in prison closing what appears to be the final chapter on this self-driving car scandal. The court also levied a $95,000 fine and ordered over $750,000 in restitution paid to Waymo.

Lessons Learned

Trade secret owners need to be alert about protecting their IP and data against departing employees. To be protectable as a trade secret, it needs to be treated as such, with electronic and physical security. Access should be limited to a need to know basis. Huge downloads should be detected before employees leave a company, not after. As well, companies also need to take measures to protect trade secrets against collaborators, since there is a risk of misuse, particularly after a collaboration ends. More information about identifying and enforcing trade secrets can be found here.

Honest employees also need to protect themselves against inadvertently becoming a target of unfounded trade secret enforcement by their former employer. Departing employees are allowed to use their general skills and knowledge at a new job. They are not permitted to take proprietary information from their company. All company devices and information (paper and electronic) must be returned to the company. There is no scope to keep company materials for one's own personal use.

Trade secret protection needs to be proactive. Employers need to set clear expectations and obligations to employees. Communication between employers and employees can avoid misunderstandings after an employee departs. Companies also need to protect themselves against commercial collaborators misusing trade secrets and other IP. Companies that suffer a trade secret theft have to move quickly and forcefully to enforce their rights.

help you.