Protecting Trade Secrets in the Autonomous Vehicle Supply Chain Continuum

Insights
9.24.18

An autonomous vehicle (AV) is driving with its passenger when suddenly a child steps into the street. The AV has a choice: hit the child or swerve into oncoming traffic risking the life of the passenger and possibly others. Tragically, the AV hits the child.

We all anguish over the human tragedy presented by this scenario. The consequences will reverberate in countless directions, one of which is certain litigation. Questions will be asked, such as "Did the vehicle spot the child, or did it hit the child because it malfunctioned?" and "If it spotted the child, did the vehicle perform as it was programmed to perform?" As the litigation proceeds, time will be spent examining the vehicle's design, programming, and functionality. Information will be disclosed, and many different players will regard this information to be their trade secrets. Why? "Among the many technologies which make autonomous vehicles possible is a combination of sensors and actuators, sophisticated algorithms, and powerful processors to execute software."

As has been true for non-automated cars, AVs will contain numerous parts from a variety of original equipment manufacturers (OEMs). OEMs must think ahead and take steps to protect their trade secrets in the supply chain continuum. How can they do this? There are two main considerations:

It all starts at home.
If you want to stop others from misusing or cavalierly disclosing your trade secrets, make sure you are protecting these secrets yourself. Implement a trade secrets protection program. Identify your secrets and threat them as such. Identify threats. Require your employees to sign confidentiality agreements and restrictive covenants. Implement appropriate security policies and procedures. Train your employees. Assemble a team responsible for ensuring compliance. Implement suitable security restraints. Litigate when necessary.

Look outward.
Just as your organization must get its internal trade secrets house in order, it must likewise look outward to identify and address external threats**.** Conduct due diligence regarding external business partners to ensure they have suitable protections in place. Look at their policies, procedures and financial health. Assess their history, if any, of intellectual property theft. Ensure they have appropriate contractual restraints with their employees, and while you are at it, make certain your contracts with your partners include adequate protection. Clearly identify your confidential information, prohibit unauthorized use and disclosure, and require notice of any efforts

confidential information, prohibit unauthorized use and disclosure, and require notice of any efforts to obtain your confidential information by way of subpoena so that you have a sufficient opportunity to seek a protective order. Require segmentation of manufacturing processes and silo information where possible. Limit your partner's ability to subcontract when appropriate, and provide yourself with the right to audit or inspect your partner's procedures.

The bottom line:
Your company is in business to make a profit. If you depend upon external business partners to sell your product or incorporate it into an end product, your ability to profit can evaporate if others obtain your secrets. As players in the AV industry, particularly if you are a start-up, you will be racing to market. In your haste, do not overlook steps essential to protect your intellectual property. Instead, ensure you cross the finish with adequate trade secret protections in place.

If you have questions or concerns regarding how companies in the AV industry can best position themselves to avoid liability for a cyber breach, contact Mike Greco or any member of our Autonomous Vehicles Practice Group.

Related People

Michael R. Greco
Regional Managing Partner
303.218.3655
Email