Watch for the Fox in Your Henhouse: Gig Companies at Risk

Insights
3.28.17

Intellectual property threats (IPT) to companies participating in the gig economy may be greater than those experienced by traditional business. While this may seem self-evident to some, reflection on the matter confirms to the rest of us that the gig sector is the more likely to only utilize internet platforms to deliver services or goods with innovative technology and digital strategies. This fact, when combined with the fast-paced advancement of cloud technology and the Internet of Things, requires gig companies to remain aggressive in operational matters and on the cutting edge of progress.

Theoretical conjecture or real-life risk?
IPT are real and should not be disregarded as an imaginary lark. By example, Waymo, LLC sued Uber under the Defend Trade Secrets Act (DTSA) last month alleging certain self-driving car technology trade secrets had been stolen. According to the complaint filed in a federal court in San Francisco, a month after leaving Waymo's employ, Anthony Levandowski, a former manager, created a new company called "Otto." Less than six months later, Uber purchased Otto to acquire its proprietary laser sensors to guide self-driving cars system (LiDAR).

Before leaving Waymo, the company alleges Mr. Levandowski downloaded 9.8 GB of highly confidential data, inclusive of LiDAR circuit board designs, and attempted to forensically conceal his unauthorized access and file removal. According to Waymo's complaint, there were other employees who later followed Levandowski to Otto, taking with them additional Waymo proprietary information related to LiDAR, including supplier lists and highly technical information regarding LiDAR components. Waymo claimed it learned of the scheme when it received an inadvertent email from a vendor containing component machine drawings of an Uber LiDAR circuit board that bore striking similarity to Waymo's LiDAR system and allegedly infringed on several of its technology patents. Having devoted seven years of resources to research and develop the LiDAR system, Waymo instituted the lawsuit to prevent its competitor from allegedly misappropriating and infringing on Waymo's technology and to recover associated damages. Uber denies the allegations, calling them a "baseless attempt to slow down a competitor." Although it hasn't filed a formal, legal response to the lawsuit, reports indicate that Uber has several planned defenses to the allegations.

Implementing a Trade Secrets Protection Program
It behooves every gig company to develop a trade secrets protection program to ensure it is well-positioned against corporate espionage and can successfully pursue litigation against wrongdoers.

Key to the program is identification of all trade secrets and confidential information to be protected. Once identified, you should identify what individuals (employees or independent contractors) have access to it so appropriate security and control protocols can be developed.

Control & Manage Access

Diligence should be required on any individual with access to a company's trade secrets and confidential information, including consideration of background screening checks in accordance with applicable laws to determine qualification for security clearances. In terms of physical and technology environments, the gig company should develop access and security protocols, surveillance measures, monitoring procedures, password/log-in/encryption protections, audit methods, and systemic reviews wherever trade secret/confidential information is housed.

Execute Necessary Legal Documents

Based on how each individual interacts with the information dictates what legal documents are needed. For example, if the person is involved in the invention process, the company should consider using an assignment of invention agreement, providing any required legal notifications. In addition, for all individuals interacting with trade secrets, non-competition, non-solicitation, and confidentiality agreements should be in place. If the individual is employed by a vendor, supplier, or subcontractor, the gig company should ensure appropriate confidentiality protections are included in contracts. For gig workers, agreement to equivalent restrictive covenants is important.

Review Electronic Footprint of Any Individual Departing Service

Anytime a person with access to trade secrets/confidential information departs service of a gig company, that individual's electronic footprint should be reviewed. Oftentimes those departing will take something beyond their personal belongings with them when they leave. By reviewing the six-to-nine month period preceding a departure, the company can identify what information was accessed and then determine whether there is any indication of a breach of confidentiality or interference with trade secret information. Any activity out of the individual's normal responsibilities should be closely examined as well as frequency in accessing the same type or category of information. With this information in hand, the company should consider where the individual next lands in their career to ascertain whether the situation should be reviewed any further. If nefarious conduct is uncovered, prompt review by legal is critical to identify next steps and ensure the gig company's rights are promptly asserted.