Insights: Alerts

5 Key Takeaways: IP Aspects of a Product to Market Timeline: A Comprehensive Look at Protecting the IP of a New Product

NOVEMBER 8, 2017 Written by

Kilpatrick Townsend partner **Karam Saab** recently presented to the Association of Corporate Counsel Denver Chapter on "IP Aspects of a Product to Market Timeline: A Comprehensive Look at Protecting the IP of a New Product."

Key takeaways from his presentation, include:

- Ahead of forming a relationship with another company with which confidential information will be exchanged, consider filing patent applications on novel aspects of your company's developments that will be disclosed as part of the relationship. Establishing an priority date ahead of the relationship being formed can help preclude the other company from claiming any portion of ownership.
- Consider filing design patents on non-functional portions of your company's products even for products not generally considered to be aesthetic in nature (e.g., unmanned aerial vehicles). Design patents can present a cost-effective route for stopping knock-off and copycat products.
- When negotiating a non-disclosure agreement with another company, pay particular attention to residual clauses. Residual clauses typically allow for confidential information retained in the unaided memory of the receiving party to be used for any purpose, thus creating a potential hole in the non-disclosure agreement for the party that is revealing significant amounts of confidential material.
- Pay attention for limitations on IP indemnification clauses. The protection of an IP indemnification clause can be undermined by a limitation on liability clause that limits a party's aggregate liability, such as to fees paid in respect to a specific portion of a product or service.
- If software is involved in the transaction, ensure that open source code is addressed. Specifically address whether the party creating the software is making any representations or warranties regarding the presence of open source code. Consider having an audit performed to scan for open source code, which may have been inserted by an employee passing the code off as his own. Ensure that distribution of the software complies with the software license under which the open source code was obtained and that the proper attributions are included with software that includes open source code.