Contributed Article

Trade Secret Enforcement and Compliance

By David Chun and Patrick Sinclair (Ropes & Gray LLP)

The importance of intellectual property ("IP") rights is well known today. IP rights are an essential element for maintaining control over a new product or invention, and may even be used to protect a corporate image. These protections not only foster additional invention, they can also be used to ward off competitors and imitators.

Today, particularly for those companies that operate across international borders, the management of IP rights is already an integral part of everyday business. Taking patents as an example, in recent years companies have filed hundreds of thousands of patent application in the United States Patent and Trademark Office. These patents then become the subject matter of the thousands of patent litigations that are filed each year in United States Federal District Courts and in the International Trade Commission ("ITC"). In large part due to the sheer volume of patent activity over many years, the process for obtaining and enforcing patent rights are today reasonably well established. As a result, companies can reasonably understand and address patent related risks and rewards. The same can also generally be said of copyright, trade mark and even trade dress protections.

Where the waters are often muddied, however, is in the realm of trade secrets. This is because the laws that define what a trade secret is and how it may be protected varies from country to country, from state to state (in the U.S.), and in the particular facts and circumstances. A case involving a former R&D employee who moves to a competitor company is very different from a case involving a corporate data breach by a malicious third party hacker. The complexity for trade secret issues is compounded by the fact that trade secret violations or economic espionage cases can even result in criminal investigations and penalties.

Further, in recent years there have been an increasing number of trade secret actions involving activities that span across both Korea and the United States. Indeed, some of these have been high profile and involved very large damages awards or fines.

A few recent trends and developments provide some context for this trend:

Intellectual Property Task Force

In 2010, the U.S. Department of Justice established a Task Force on Intellectual Property to address the increased threat to American businesses due to intellectual property crimes. The Attorney General emphasized that threats from foreign entities was a primary concern. Simply put, the initiative by the Department of Justice resulted in enhanced focus and greater allocation of manpower and other resources to prosecute IP related crimes - more agents, more prosecutors and more funding.

Expansive Reach

The United States can investigate crimes based on foreign activities, so long as there is a sufficient nexus to the United States. As can be seen in the news regarding the recently announced investigation into the activities of Fédération Internationale de Football

Association (FIFA), prosecutors can exercise broad jurisdiction even where individuals and corporate entities are outside of the U.S. Indeed, the level of cooperation between international law enforcement authorities in these contexts continues to increase over time. We can also see broad jurisdiction in other contexts, including in the ITC where trade secret misappropriation actions can be brought in some circumstances even where the misappropriation took place outside of the United States.

Cooperation with prosecutors

Private parties often cooperate with authorities in investigations. In the context of trade secrets, an aggrieved party (who likely is a competitor) might even bring evidence of the trade secret theft to a federal prosecutor to help initiate the investigation and to prove that a theft had occurred.

In light of the recent trend in trade secret enforcement actions, companies are increasingly turning to IP compliance guidelines. While many companies already have general ethical or corporate conduct related compliance guidelines, or guidelines relating to the handling of the companies' own information, a robust policy relating to the treatment of third party confidential information is not prevalent.

State of the art IP compliance guidelines generally include three main components:

1. IP Concepts

Guidelines should explain basic concepts relating to patents, trademarks, copyrights and trade secrets. Through education of basic concepts, individuals will be able to better spot potential issues and avoid wrong-doing.

2. Interactions with Third Parties

The greatest risk to companies stems from interactions with third parties who might have confidential information. Guidelines should include requirements for the receipt, storage, access and dissemination of third party confidential information. Guidelines should also include diligence requirements for the hiring or retention of new employees or agents (e.g., consultants, regional sales agents) and for dealings with suppliers, distributors or vendors.

3. Model provisions

Companies should include model contractual provisions for employees that apply to specific situations. Examples include model non-disclosure provisions, contractual language for use with consultants, or a due diligence checklist for use when researching a potential new hire.

Because a company might be on the hook for the activities of its agents, IP compliance guidelines should also apply to the company's agents in addition to the company's own employees. And, as with all compliance programs, regular training, monitoring and auditing will help the program be successful.

***David Chun**, US Lawyer & Foreign Legal Consultant, is one of the founding partners of Ropes & Gray LLP's Seoul office. He focuses his practice on litigating patent infringement, trade secret misappropriation and copyright infringement matters in U.S. courts and in connection with government enforcement actions.*
David is consistently recognized as a leading attorney in U.S. patent litigation by publications including Chambers. He is an adjunct professor at Georgetown University Law Center and also a director of the Korean Intellectual Property Lawyers Association (KIPLA).

***Patrick Sinclair** is a partner of Ropes & Gray LLP and a Registered Foreign Lawyer in the Hong Kong office. Patrick was a federal prosecutor in the U.S. Attorney's office for the Eastern District of New York (2007-2014) and was appointed as Deputy Chief of General Crimes.*
His practice is focused on white collar criminal defense, internal investigations, and risk assessment in the anti-corruption and sanctions spaces.