

Best Practices in Intellectual Property Protection: Are Your Asian Suppliers Protecting Your Interests?

By Wee Leong Ng, San Francisco Centre Director, SPRING Singapore

Protecting intellectual property (IP) via legal documents is only a part of a robust IP protection strategy. Discipline in handling sensitive information is equally important. Sourcing teams often face the challenge of balancing the requirement to lower manufacturing costs with the requirement to protect valuable IP. Does this need to be a tradeoff in all cases? The answer is no. This paper looks at methods used by Singaporean-headquartered suppliers to protect sensitive data, even in countries where IP theft risk is considered high.

The first step in any IP protection strategy is to understand the legal infrastructure and available protections in the region where the product will be manufactured. Typically, this is best handled by corporate counsel or a firm specializing in IP management in the selected region.

Overview of IP Protection Culture in Singapore

Singapore represents an excellent example of IP protection best practices at a government level. Singapore's strong focus on intellectual property protection earned it the top ranking for IP protection in the World Economic Forum's Global Competitiveness Report for 2009 – 2010 (http://www3.weforum.org/docs/WEF_GlobalCompetitivenessReport_2009-10.pdf). The World Intellectual Property Office (WIPO) chose Singapore for the location of its first Asian regional office in June 2005 (<http://www.wipo.int/about-wipo/en/offices/singapore/>).

Singapore's legal system is based on British Common Law, as is the U.S. legal system. English is the official language of business. These two elements make it relatively easy for U.S. companies to understand their available legal protections and prosecute in the event of IP theft.

The Intellectual Property Office of Singapore (IPOS) www.ipos.gov.sg, a statutory board under the Ministry of Law since April 2001, is the lead government agency advising on and administering IP laws. IPOS also promotes IP awareness and provides the infrastructure to facilitate the development of IP in Singapore. Its core services include the filing and registration of patents, trademarks, designs and plant varieties. IPOS also conducts hearings and mediations for IP disputes such as trade mark oppositions. There is also a copyright tribunal that handles disputes between copyright owners and users.

For cross border disputes, Singapore has set up an Alternative Dispute Resolution (ADR) Advisory Committee to address disputes around the world, particularly in Asia, outside of the traditional court system.

Singapore has a fully Trade-Related Aspects of Intellectual Property Rights (TRIPS)-compliant Intellectual Property Rights (IPR) legislative and administrative regime. It is also a signatory to the following international conventions:

- Paris Convention

- Berne Convention
- Madrid Protocol
- Nice Agreement
- Patent Cooperation Treaty
- Budapest Treaty
- WIPO Copyright Treaty
- WIPO Performances and Phonograms Treaty
- International Convention for the Protection of New Varieties of Plants otherwise known as the "UPOV Convention"
- The Geneva Act (1999) of the Hague Agreement concerning the International Registration of Industrial Design
- Singapore Treaty on the Law of Trademarks.

The end result is that companies doing business in Singapore have an easy-to-use system that is integrated with key international conventions for ensuring IP protection. This is reinforced by a highly ethical culture, which drives IP discipline throughout the supply chain, both in Singapore facilities and in those located in other parts of the world.

Best Practices in IP Protection Discipline

While a legal system which supports prosecution of those stealing IP is an integral part of IP protection, the best defense is to create systems which minimize the likelihood of IP being stolen.

Representatives from seven Singapore-headquartered electronics manufacturing services (EMS) and precision engineering companies discussed the checks and balances they use in protecting their customers' IP.

The interviewees are:

Heng Teck Yow, vice president business development at **CEI Contract Manufacturing Limited**. CEI (www.cei.com.sg) is an electronics manufacturing services (EMS) provider with facilities in Singapore, Indonesia, Vietnam and China.

Ronald Lilly, vice president sales & marketing, **Forefront Medical Technology Pte Ltd**. Forefront Medical Technology (www.forefront.sg) focuses exclusively on the medical device industry and has extensive expertise with contract manufacturing, injection molding, extrusion, blow molding, device assembly and packaging of specialty medical disposable devices. Manufacturing facilities are located in Singapore and China. A technical sales office is located in Farmington, CT.

Jordy Teo, senior business development & account manager, **HISAKA (Singapore) Pte Ltd**, a subsidiary of HISAKA Holdings Ltd. HISAKA (www.hisaka.com.sg) is an automation solutions provider specializing in mechanical motion products. It has facilities in Singapore, Malaysia, Thailand and China.

Thomas Ho, operations manager at **Inzign Pte Ltd**. Inzign (www.inzign.com) is a Singapore-based plastics contract manufacturer of medical devices.

Tee Soon Ann, vice president of business development at **Nestronics Limited**. Nestronics (www.nestronics.com.sg) is a Singapore-headquartered EMS provider with subsidiary plants in Malaysia.

Malvin Ng, manager, business development, **PLC Industries, Pte Ltd**. PLC Industries (www.plc.com.sg) is a precision manufacturer of highly intricate products for medical and photonics industries.

Willy Koh, managing director. **Racer Technology Pte Ltd**. Racer Technology (www.racer.com.sg) specializes in manufacturing high quality precision medical devices, plastic components and complete unit assembly. It has facilities in Singapore, the U.S., Malaysia, Indonesia and China.

Based on overall comments, there are several key elements to creating a robust system including:

- Execute non-disclosure agreements (NDAs) with all suppliers
- Control internal access to sensitive documents
- Segregate teams associated with competitive products
- Control supplier access to detailed information
- Control data movement within the facility
- Ensure all persons and suppliers handling sensitive information understand their responsibility to protect that information.

All of the respondents execute NDAs with their suppliers. But, all also have additional protections built into their systems for handling sensitive information.

CEI: We execute NDAs with all our suppliers, but as added insurance only piece part drawings are sent to suppliers. No supplier receives a drawing package capable of forming an assembly.

Forefront Technology: By the nature of our specialty business, it's very important to us to protect our customer's confidential information. NDAs are established early on, as a necessary step, to safeguard this information. Customer names are never mentioned to other customers, as a rule. Information that is shared with suppliers is coded with a specific internal project reference designator. Customer names, products, part numbers or specific references are removed. In addition, we never purchase all of the product components from a single source.

HISAKA: We execute NDAs and convert drawings shared with suppliers to remove information that is not necessary for their activities.

Inzign: We ensure that an NDA is not only signed and acknowledged, but also clearly understood by any supplier who will receive sensitive information. Our company ensures that all our employees conform to strict IP protection practices. All new employees hired by Inzign sign an NDA where they agree not to have unauthorized copies of software, drawings etc. All violators are subject to disciplinary actions which may include termination of the employee's services from the company.

Nestronics: We execute NDAs with our suppliers prior to any document issuance and we also limit our staff's access to customers' sensitive documents. All documents are controlled through our document control department and are only issued to staff members who are involved in the specific projects.

PLC Industries: On secondary processes, we either remove some of the critical information or issue an entirely new drawing. All documents are controlled copies and no originals circulate on the production floor. For customers with significant concerns about sensitive data we assign a dedicated work cell team that only works for that customer.

Racer: We regulate use of portable storage devices. Many corporations have lost sensitive data through illegal usage of such devices to download sensitive data. Hence, we have the compelling need to administer and control the usage of these devices within the corporate environment. On one hand, it is important that all sensitive data stored on the portable storage devices are encrypted. It is equally important to ensure that unauthorized devices are disabled. We have implemented protection which prohibits unauthorized portable storage devices from accessing sensitive and confidential information in our enterprise IT environment. This system also allowed us to create a list of authorized users associated with specific data. This is important because devices are now so small that it can be difficult to physically check individuals to see if they are carrying one. We see this as less of a sensitive issue in Singapore and Indonesia. However, in China and Malaysia, we've put in more security and use the most up-to-date hardware and software. We've got a strategic relationship with Trek for this activity. In exchange for our user feedback on desired improvements, they give us preferred pricing and access to products before they launch them on the market. It is a win-win relationship.

About SPRING Singapore

SPRING Singapore (www.spring.gov.sg) , which is under the Singapore Ministry of Trade & Industry, is the national enterprise development agency responsible for helping Singapore enterprises grow. It works with partners to help enterprises in financing, capability and management development, technology and innovation, and accessing new markets.

As the national standards and accreditation body, SPRING develops and promotes an internationally-recognized standards and quality assurance infrastructure that builds trust in Singapore enterprises, products and services, thereby enabling their global competitiveness and facilitating global trade.

Corporations that are interested to collaborate with Singapore enterprises are welcome to contact SPRING for assistance. U.S. offices are located in Chicago and San Francisco. For more information, email Wee Leong Ng at NG_Wee_Leong@spring.gov.sg.