Inside India’s IP Market: a Guide
2024
Managing Infringement Threats Across the Supply Chain
Inside India’s IP Market: a Guide
2024

The first edition of Inside India’s IP Market provides invaluable on-the-ground intelligence and analysis on a range of trademark and patent topics, covering every stage of the IP lifecycle and the unique challenges and opportunities facing rights holders in India.

Generated: April 2, 2024
The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. Copyright 2006 - 2024 Law Business Research
Managing Infringement Threats Across the Supply Chain

Daizy Chawla, Shrimant Singh and Samridh Ahuja
S&A Law Offices

Summary

INTRODUCTION
COMMON THREATS IN OUTSOURCING AND OEMS
MANAGING IPR INFRINGEMENT THREATS
ADDITIONAL CHALLENGES AND CONSIDERATIONS SPECIFIC TO INDIA
CASE STUDIES: MANAGING IPR INFRINGEMENT THREATS IN INDIA
CONCLUSION
INTRODUCTION

In today’s world without boundaries, businesses are characterised by rapid technological advancements, a unique factor on a global scale and fierce competition, thus making intellectual property (IP) the cornerstone for the growth and success of a business. IP rights play a critical role in protecting innovation and fostering economic growth. Industries such as outsourcing and original equipment manufacturers (OEMs) are key drivers of the global supply chain. With more and more cross-border collaborations and marketplaces, the industries expand, and along with it, the risks of IPR infringement also increase.

India being a preferred destination for outsourcing and OEMs, India has emerged as one of the world’s leading destinations for manufacturing and outsourcing, attracting businesses from various industries. In simple terms, outsourcing refers to contracting out specific business processes to third-party service providers, allowing companies to reduce costs, access specialised skills and focus on their core competencies. India has been a preferred outsourcing destination due to its skilled workforce, cost advantages and robust technology ecosystem. OEMs, on the other hand, are companies that design and manufacture products, often under the brand of another company. India has emerged as a global OEM hub, especially in industries such as electronics, automotive and pharmaceuticals.

With this exponential growth in outsourcing and OEMs in India, the concern for international IP owners, including brands and inventions, has also grown regarding the adequate protection and enforcement of their IPs in India. The vast and complex Indian marketplace further increases this concern of international IP owners. This article highlights the areas of concern and gives basic guidelines to avoid or neutralise any such threats to IP while dealing with outsourcing and OEM partners in India.

COMMON THREATS IN OUTSOURCING AND OEMS

1. Counterfeiting and piracy: the outsourcing and OEM units are often found to be the leaking spots and, in some cases, involved in counterfeit goods, software piracy and IP thefts. If strict checks are not in place, counterfeit products and piracy severely harm brand reputation and innovative aspects, and directly eat away profits of the IP owners.

2. Data security breaches: outsourcing and jobs to OEM partners often involve sharing sensitive information with these partners in India. Data breaches lead to theft of proprietary information, trade secrets and customer data, potentially leading to IPR infringement. One of the toughest to implement is the data confidentiality and security at the outsourcing or OEM partner and the real-time evaluation and change in the SOPs are often required.

3. Contractual ambiguities: it is not uncommon for a standard contract or agreement to be replicated for several years leading to unclear contractual agreements, which gives escape routes for IP dilution. It is crucial to precisely define ownership and strict usage guidelines to ensure protection of IP at outsourcing and OEM partners.

4. Supplier/sub-vendor/partner violations: the subcontracts are also found to breach on IP.

5. Technological advancements: the IP owners will have to keep up with the updates on data protection, encryption and managed access control – lag on the encryption
technique or data security protocols are often found to be reasons for data breach. Outsourcing and OEM partners may require frequent updates and adaptations as part of their contract and/or directly supervised or part of due diligence by the IP owner.

**MANAGING IPR INFRINGEMENT THREATS**

Effective management of IPR infringement threats in outsourcing and OEMs requires a comprehensive approach that involves legal, contractual, technological and organisational strategies.

**CLEAR AND ROBUST CONTRACTS**

- Define ownership: the contract must clearly outline who owns the intellectual property developed during the outsourcing or OEM engagement. It should include all IP that is being transferred for specific purposes and use. These provisions should include copyrights, patents, trademarks, designs, trade secrets and/or any information that is marked proprietary or confidential.

- Usage rights: these particularly define rights as well as limitations regarding usage of intellectual property shared with the outsourcing or OEM partners. This should cover how the IP can be used, modified or sublicensed/subcontracted. A well-defined usage right, along with the duty to monthly provide a compliance report or certificate, ensures continued sensitivity and importance to the IP.

- Non-disclosure agreements (NDAs): include NDAs in contracts to ensure that sensitive information remains confidential, reducing the risk of data breaches and IP theft. Here a balance is to be maintained so that the functionality of the outsourcing or OEM partner is not hindered while at the same time any proprietary information should not be disclosed beyond need-to-know basis. Clear marking of sensitivity and confidentiality of the shared data or information is a must. IP owners may also choose to have hierarchical confidentiality defined for different types of information or IPs.

**DUE DILIGENCE IN PARTNER SELECTION**

- Background checks: before entering into an outsourcing or OEM agreement, thoroughly vet potential partners and suppliers to ensure they have a strong track record of IP protection. A continued IP protection audit can be made part of a periodical or surprise inspections at the outsourcing and OEM partners.

- Reputation assessment: consider partners’ reputation and adherence to ethical standards in the industry to mitigate the risk of IPR infringements.

- Ongoing due diligence: in addition to the above, frequent due diligence or audit exercise for at least initial three to five years has been found to be an effective way to build trust and to clearly communicate to outsourcing and OEM partners about expectations of the IP owners.

**TECHNOLOGY SOLUTIONS**

- Data encryption: robust data encryption methods should be implemented to protect sensitive information during its transfer and storage.

-
Access control: strict access control measures should be implemented to restrict unauthorised access to IP, sensitive information and/or confidential data.

- Digital rights management (DRM): use DRM tools to protect digital content, limiting unauthorised distribution and reproduction.

EMPLOYEE TRAINING AND AWARENESS

IP owners should indulge in periodical training sessions for employees to raise awareness about IPR, data security and best practices. There is a need to foster a culture of IP protection by encouraging employees to report any suspicious activities.

INTELLECTUAL PROPERTY AUDITS

- Well-defined and exhaustive IP audits are instrumental to assess the state of your IP and identify any vulnerabilities or potential infringements. Special attention should be given to ensuring transparency of such reports, and self-audit or auditor appointed by the outsourcing or OEM partner should be avoided if possible.

- Immediate corrective actions based on the audit findings are a must not only to ensure correction at the partners’ end but also to give a clear message of adverse implications in case of deviation from the IP protocols/terms.

ENFORCEABLE LEGAL MEASURES

- Be prepared to take legal action against infringers. Have a legal team or firm appointed in India and develop a strategy for addressing IPR violations. An active legal team is found to be instrumental in preventing any malpractice at the outsourcing and OEMs end.

- Register all IPs in India, including patents, trademarks, designs and copyrights – a basic and obvious step but often found overlooked by IP owners while doing business or having markets in India.

CYBERSECURITY PROTOCOLS

- Invest in robust cybersecurity protocols to safeguard against data breaches and unauthorised access to intellectual property.

- Regularly update security systems to stay ahead of evolving threats.

DOCUMENTATION AND RECORDS

- An SOP on handling documentation and records is a must. Maintain thorough records of all IP-related transactions, communications and agreements.

- Proper documentation can serve as evidence in the case of disputes or legal action. Lack of evidence often proves fatal in an infringement matter, just like any litigation.

ALTERNATIVE DISPUTE RESOLUTION (ADR)

Consider ADR methods, such as mediation and arbitration, as a means to resolve disputes relating to IP handling and transactions more efficiently and cost-effectively than going to court.

CONTINUOUS MONITORING AND EVALUATION
Continuously monitor IPR activities, contractual compliance and the security of sensitive information.

Regularly evaluate and update IPR protection strategies based on emerging threats and changes in the business environment.

ADDITIONAL CHALLENGES AND CONSIDERATIONS SPECIFIC TO INDIA

Managing IPR infringement threats in India comes with specific challenges and considerations:

- Legal framework: India has made significant progress in strengthening its legal framework for IPR protection. Understanding local laws and regulations is crucial for effective IPR management.
- Enforcement: while India has improved IPR enforcement, challenges still exist, and the legal process can be time-consuming. Companies must be prepared for potential legal battles.
- Local partnerships: building strong local partnerships and relationships can help mitigate IPR infringement threats. Local partners and continued relationships with a local reputed law firm can often navigate the legal and business landscape more effectively.
- Cultural differences: understanding cultural norms and business practices in India is essential. Misunderstandings or miscommunications can lead to contractual issues and IPR disputes. At times, the prevalent practices in the industry at large or the customary interpretation of certain provisions or a judicial precedent specific to Indian business practices and laws comes as a surprise to an international IP owner. An effective legal counsel since the inception of the relations in India is therefore instrumental in having a good grip over complex business practices in light of the prevalent laws, interpretation by honourable courts, etc.
- Government initiatives: stay informed about government initiatives and incentives related to IPR protection in India. Taking advantage of these programmes can greatly enhance your IPR protection strategy.
- Geopolitical factors: keep an eye on geopolitical factors that may impact IPRs, such as trade agreements and international relations, as they can influence the legal and business environment.

CASE STUDIES: MANAGING IPR INFRINGEMENT THREATS IN INDIA

To illustrate effective strategies for managing IPR infringement threats in outsourcing and OEMs in India, we can look at two hypothetical case studies.

CASE STUDY 1: SOFTWARE DEVELOPMENT OUTSOURCING

A US company dealing in software development and software products outsources its coding, research and programming tasks to an Indian IT services provider. To manage IPR infringement threats, the US company must take care of:

- Clear contracts: ensure that the outsourcing contract explicitly states that all the codes and logic developed belong to them, and the Indian service provider has no rights to unauthorisedly use or distribute the codes and/or logic.
• Data security: both parties agree to implement stringent data security measures, including encryption, access controls and regular security audits.

• Legal support: the US company should maintain an active legal team in India to quickly address any potential IPR infringements or disputes.

• Regular audits: periodic IPR audits should be conducted to evaluate compliance and security. Any vulnerabilities identified are addressed promptly.

CASE STUDY 2: ELECTRONICS OEM IN INDIA

• An Indian electronics manufacturing company produces components for a multinational electronics brand. To manage IPR infringement threats, the following should be considered:

• Clear OEM agreements: the agreement outlines that all designs and technology provided by the multinational company are solely for manufacturing purposes and cannot be used for independent production or shared with other clients.

• Secure manufacturing facilities: the Indian OEM invests in state-of-the-art security systems, including access controls and surveillance, to prevent unauthorised access to sensitive designs.

• Regular IP training: employees are regularly trained on IPR protection and are encouraged to report any suspicious activities.

• Due diligence in partner selection: the multinational company conducts thorough background checks before selecting the Indian OEM partner, ensuring their commitment to IPR protection.

CONCLUSION

The outsourcing and OEM industries in India offer numerous benefits to businesses, but they also come with significant IPR infringement threats. To successfully navigate these challenges, it is crucial for companies to implement a holistic approach that encompasses legal, contractual, technological and organisational strategies.

By establishing clear and robust contracts, conducting due diligence in partner selection, employing technological solutions, fostering a culture of IPR awareness and being prepared to enforce legal measures, companies can protect their intellectual property rights in the dynamic Indian business environment. Moreover, understanding the unique challenges and considerations of the Indian market is essential for effective IPR management. Through proactive and comprehensive strategies, businesses can not only mitigate IPR infringement threats but also thrive and innovate in the outsourcing and OEM landscape in India.
Daizy Chawla
daizy@sandalawoffices.com
Shrimant Singh
shrimant@sandalawoffices.com
Samridh Ahuja
samridh@sandalawoffices.com

Plot Nos. 5, 6 & 7, Udyog Vihar, Phase IV, Sector 18, Gurugram, Haryana 122015, INDIA

Tel: +91 11 46667000

https://sandalawoffices.com/

Read more from this firm on WTR