

Offshoring to India: Are Your Trade Secrets and Confidential Information Adequately Protected?

Sonia Baldia



Sonia, based in Washington, DC, counsels corporate clients in onshore and offshore outsourcing, cross-border technology transfers, strategic alliance arrangements, intellectual property acquisition, development, marketing and distribution agreements, licensing arrangements, and consulting services agreements. A significant portion of her practice involves India-related matters.

202 263 3395

sbaldia@
mayerbrown.com

Despite recent growth in other emerging markets, India continues to be the number one destination for outsourcing services involving information technology and business processes (“IT/BPO services”). In recent years, moreover, a new model of global sourcing to India known as knowledge process offshoring or “KPO” has taken hold in addition to the remarkably successful Indian market for IT/BPO services, with India emerging again as the global KPO “hot spot.” KPO involves the offshore outsourcing of knowledge-driven or “high end” processes that require specialized domain expertise, including such varied areas as R&D, insurance underwriting and risk assessment, financial analysis, data mining, investment research, statistical analysis, tax preparation, engineering and design, animation, graphics simulation, medical services, clinical trials, legal services, and more. As offshoring of services to India moves up the value chain from IT/BPO services to KPO, protection of intellectual property (IP), including any trade secrets and confidential information, that may be transferred or created in India becomes an even more critical concern for the offshoring customer. IP concerns must be addressed knowledgeably to achieve and maximize the benefits and strategic incentives the offshoring model offers without losing control of critical customer IP. This article raises some of the key issues that any offshoring customer should carefully assess so as to mitigate the risks associated with offshoring trade secrets and other confidential information to India.

When offshoring a “high end” process or functionality to India, often much of the knowledge transferred offshore (for example, source code, formulae, designs, specifications, or experimental data) is confidential in nature and generally not suitable for local registrations in the form of patents. It, therefore, becomes critical for the US customer to seriously consider – before it begins the offshoring process — how it will best protect this information to maintain its competitive advantage. A primary concern for a US customer should be the Indian service provider’s ability and willingness to safeguard the customer’s trade secrets and other commercially valuable confidential information against misappropriation, misuse, unauthorized disclosure, sabotage or theft.

India’s Existing Legal Framework for Trade Secrets

In the US, trade secrets are afforded statutory protection, both at the federal and state levels, with meaningful civil and criminal remedies to counter the misappropriation of trade secrets, including compensatory and punitive damages, injunctive relief, and attorneys’ fees. That is not the case in India. India provides no statutory or other legal protection of

trade secrets. This non-legal environment presents a number of challenges concerning trade secret protection and enforcement and can jeopardize a US customer's IP unless it carefully employs certain contractual mechanisms that are enforceable in India. In India, parties must primarily rely on contracts to protect trade secrets. Indian law does recognize the common law tort of "breach of confidence" irrespective of the existence of a contract. But the tort's utility is limited in an offshore sourcing context because the duty of confidence at issue can be enforced only against a party that is either a fiduciary to the US customer or in an employer-employee relationship with the complaining party. Also, the duty arguably only extends to the unauthorized disclosure of confidential information to a third party and does not prevent the recipient's own "misappropriation" of the information.

Perils of Subcontracting

Consider the following hypothetical involving an Indian service provider that has engaged a subcontractor in India to perform the offshored services for a US customer. If the Indian subcontractor discloses or misappropriates the US customer's trade secrets or confidential information, the US customer has neither a breach of confidence claim against the subcontractor nor a breach of contract claim, unless the US customer has contracted directly

This non-legal environment presents a number of challenges concerning trade secret protection and enforcement and can jeopardize a US customer's IP unless it carefully employs certain contractual mechanisms that are enforceable in India.

with the subcontractor, which is typically unlikely. The contract between the US customer and the Indian service provider might well hold the service provider liable for damages caused by the subcontractor's inappropriate disclosure, but that cause of action still does not directly address

or foreclose the subcontractor's past and possibly future misconduct. Essentially, the US customer is left without a direct remedy against the Indian subcontractor and without an immediate legal means to effectively stop the disclosure.

Employee Misconduct

This concern with third-party subcontractor misconduct unfortunately also exists with respect to the misconduct of employees and ex-employees of the Indian service provider. Surveys reveal that a majority of instances of data misconduct arise from employees or ex-employees of a service provider. Recent instances reported in international media involving theft of trade secrets of western companies offshoring to India further illustrate the gaps in India's IP law that expose the vulnerability of IP in offshore transactions. In 2002, an ex-employee of an Indian software vendor, Geometric Software Solutions Ltd., was attempting to sell proprietary software source code owned by SolidWorks, a US client of the person's ex-employer, to the US client's competitors. Even though the ex-employee was caught red-handed in a sting operation, he could not be effectively prosecuted in India because the source code was considered a trade secret and Indian law did not recognize "misappropriation" of trade secrets and the US client did not have any contractual arrangements with the ex-employee whereby it could directly enforce its rights against the ex-employee. Similarly, in

2004, an employee at an India-based software development center of a US customer, Jolly Technologies, misappropriated portions of the company's source code by allegedly uploading and shipping files that contained source code for a key product to her personal Yahoo e-mail account. The theft was detected in time to prevent the employee from distributing the stolen code but the US customer also could not successfully prosecute the employee because of the same gap in Indian IP law. These cases have drawn close scrutiny and served as a wake-up call to the global sourcing community as well as the Indian outsourcing industry prompting Indian industry to aggressively lobby the Indian government to strengthen India's IP regime and demonstrate to the foreign investor community that India takes foreign IP more seriously.

The perils of subcontractor and employee misconduct as to IP in India are very real. It is critical, therefore, for a US customer to be aware of this enforcement gap and address it in the operative contract with the Indian service provider and in the contracts between the Indian service provider and its subcontractors.

Effective Strategies to Safeguard Trade Secrets and Confidential Information Offshored to India

DRAFTING COMPREHENSIVE CONFIDENTIALITY AND IP OWNERSHIP AGREEMENTS THAT ARE ENFORCEABLE IN INDIA

Trade secrets and confidential information must be protected through the contractual arrangement between the US customer and the Indian service provider and there should also be a contractual relationship between that service provider and its subcontractors that includes an express right of enforcement by the US customer against the subcontractors. The contract provisions should, as clearly and as effectively as possible, prohibit the wrongful disclosure and misappropriation of trade secrets and proprietary data by the service provider and the subcontractor(s); the contracts should make equally clear and expressly acknowledge the US customer's right to enforce violation of these provisions for damages and the customer's right to seek to enjoin such wrongful acts locally.

Confidentiality and non-competition covenants are enforceable under Indian law and offer a line of defense in the US customer's efforts to protect trade secrets and confidential information in India. A US customer must therefore insist upon unambiguous provisions in the operative contract that require the Indian service provider to (i) maintain the customer's trade secrets and confidential information in strict confidence not only during the term of the contract but also after termination, (ii) permit controlled access on a "need to know" basis only, including the customer's right to enforce such obligations directly against service provider personnel having access to the customer's information, and (iii) be contractually responsible and liable for any breach of confidentiality obligation or misuse of such information by itself, its subcontractors, employees or former employees. A service provider's failure to comply with the confidentiality obligations should not only permit the customer to immediately terminate the contract but also result in uncapped financial consequences to the service provider.

PERFORMING DUE DILIGENCE TO AVOID CHAIN OF TITLE ISSUES AND ENSURE PASS-THROUGH NON-DISCLOSURE OBLIGATIONS

Needless to say, because prevention is better than cure, a US customer should conduct thorough due diligence regarding the Indian service provider's track record of maintaining data security. Prior to entering into a final contractual arrangement, a US customer should perform due diligence as thoroughly as possible to make sure that the Indian service provider has written employment agreements in place with its employees and consultants addressing IP ownership and non-disclosure obligations and closely scrutinize such agreements to make sure they are sufficiently protective of the US customer's rights and interests, and are valid and enforceable under Indian law. To the extent practicable, and depending on the nature and sensitivity of the US customer's IP involved in the project, a customer should consider entering into non-disclosure and IP ownership agreements directly with the Indian service

Subcontracting by the Indian service provider can dramatically increase the IP risk profile.

provider's employees and consultants assigned to the project. By doing so, the confidentiality and IP ownership obligations should remain in force even after the employee or consultant is no longer

employed or engaged by the Indian service provider and the US customer will have contractual privity with such employees and consultants and legal standing to sue in India, as well presumably in other venues, in the event of a breach of their obligations.

IMPOSING NON-COMPETE RESTRICTIONS THAT ARE ENFORCEABLE IN INDIA

The operative contract should also include non-competition covenants that restrict the Indian service provider from using competitive technology or personnel in connection with the customer's competitors. The US customer must bear in mind, however, that India has stringent laws against overly restrictive trade practices and therefore the enforceability of a non-compete covenant is subject to a case-by-case determination and any particular terms cannot in every case be assumed to be enforceable. More specifically, the Indian Contract Act provides that a non-compete agreement will not be enforced to the extent that it restrains a person from exercising a lawful profession, trade or business. Judicial precedent under Indian law indicates, however, that an Indian court will enforce a restrictive covenant if it meets what is known as a "reasonableness" test. For example, a restrictive covenant imposed during the period of the subject's employment is more likely to be upheld than a covenant operating after the termination of employment. In *Niranjan Shankar Golikari v. The Century Spinning & Manufacturing Co. Ltd.*, the Supreme Court of India upheld a restrictive clause in an employment contract, which imposed constraints on the employee not to reveal or misuse during the period of the employment any trade secrets that the employee learned while employed. Another example of the application of the "reasonableness" test is that Indian courts also typically apply a stricter level of scrutiny to non-competition provisions in contracts for the provision of services than to contracts solely for the sale of a business or franchise agreements restraining the franchisee from dealing with competing goods, thus making the drafting of these provisions in offshoring contracts a critical and sensitive task.

ENFORCING PROPER CHECKS AND BALANCES ON SUBCONTRACTING

Subcontracting by the Indian service provider can dramatically increase the IP risk profile. Therefore, proper checks and balances should be placed on the Indian service provider's ability to subcontract any portion of the offshored services. To the extent possible, the US customer should require that subcontractors enter into contractual commitments that are directly enforceable by the US customer. At the very least, the US customer should (i) require prior approval rights with respect to all subcontractors and retain the right to review the terms of all subcontracts, (ii) require flow down of certain mandatory provisions to safeguard the US customer's rights and interests, such as data privacy, IP ownership and assignment provisions and confidentiality obligations, (iii) perform thorough due diligence with respect to subcontractors, (iv) require the Indian service provider to be contractually responsible for subcontracted functions, and (v) insist upon contractual arrangements, to the extent practicable, that maximize the customer's chances in India of being positioned legally to enforce contractual protections regarding data privacy, confidentiality and IP ownership directly against the subcontractor.

IMPLEMENTING EFFECTIVE INFORMATION GOVERNANCE MEASURES

The US customer should perform a risk assessment prior to sending any sensitive information offshore and develop and implement effective information governance strategies and internal security measures to control the access, availability and dissemination of trade secrets and confidential information in India. Key measures include (i) requiring meaningful background checks to be performed on employees and consultants engaged by the Indian service provider and assigned to the US customer's account, (ii) permitting controlled access on a "need to know" basis, (iii) managing attrition and turnover rate of employees, (iv) briefing employees on security measures and conducting exit interviews of ex-employees to remind them of continuing confidentiality obligations, (v) performing routine audits to verify a service provider's compliance, and (vi) to the extent possible, marking hard copy documents and electronic data with "confidential" or "proprietary" legends prior to placing them in circulation. In addition, because most security breaches are generated internally by employees, the US customer should require the Indian service provider to implement personnel security through a three-pronged approach of employee screening, training, and a robust disciplinary process.

ASSESSING NEED FOR LOCAL PATENT REGISTRATIONS IN INDIA

Before embarking on an offshoring transaction involving India, a US customer should determine whether to protect its IP that might be shared or created in India through trade secrets or by obtaining a local patent in India. The fundamental questions are whether to seek local patent protection for any invention that is patentable or already patented outside India that would be made available in India or for any innovation originating in India, and whether to make any subsequent global filings for any India-originated innovation. Through a well thought out patent strategy upfront, a US customer can minimize not only infringement risk but also the risk of potential loss of any global patent rights, particularly given

the differing standards of patentability worldwide. To a large extent, the patent strategy will be driven by the nature of the offshoring project and the degree of critical IP involved. For example, in a KPO in India involving research and development of chemical entities, it may be worthwhile to obtain local patent protection for the chemical entities. Similarly, in a KPO involving the manufacture of drugs in India, the customer may wish to obtain local patent protection for the drug formulations to prevent local generic companies from copying the drug. A key benefit of patent protection is that it provides the patent owner with a bundle of strong statutory rights that may be enforced against any third party in India to stop any unauthorized use of the patented technology, irrespective of the existence of any contractual or fiduciary relationship.

Furthermore, unlike in the case of trade secrets or copyrights, independent development of a patented technology is not a defense to a claim of infringement. While not usually a significant risk, a US customer in India should generally be aware that India's patent laws do empower the government to grant a "compulsory license" to a private party or a government agency under certain circumstances. India's patent laws also provide for broad "research and experimental use" exceptions whereby a third party's experimental use of a patent, even for commercial purposes, without the patent owner's consent does not constitute infringement. Finally, a US customer must keep in mind that computer programs and business methods continue to be *per se* not patentable in India, and so must be protected as trade secrets through the contractual approaches discussed above.

OTHER IP CONSIDERATIONS

As a practical way to manage the risk to IP, the US customer should (i) perform detailed due diligence of the Indian service provider upfront to evaluate the entity's track record for protecting IP, (ii) be extremely particular about which IP must truly be offshored and avoid where possible offshoring critical technology, (iii) maintain core components of the offshored IP in the US, and (iv) require frequent disclosure of work-in-progress and periodic delivery of deliverables during the course of the project to avoid being denied access to such technology in the event of a dispute or bankruptcy. To mitigate risk, businesses may adopt a "distributed R&D model" by dividing R&D responsibility among multiple entities, and sometimes even across multiple jurisdictions, but this can be an expensive operating model as additional capital and resources would be required to manage and integrate results from the various entities.

EXPLORING MECHANISMS TO MITIGATE ENFORCEMENT RISKS IN INDIA

The enforcement of the US customer's rights and remedies is always a vital concern, and those concerns can be exacerbated when dealing with an Indian service provider, particularly one that has few or no meaningful assets in the US against which any judgment could be executed. If the Indian service provider has meaningful assets located in the US and a US plaintiff successfully obtains a judgment in a court of competent jurisdiction, the judgment can be enforced against those US assets. However, even if a dispute with an Indian service

provider is adjudicated in the US, if the Indian service provider's primary assets are located in India and not in the US, the US customer must still seek redress within the Indian legal system to obtain and enforce a judgment against the Indian service provider's India-based assets.

Jurisdiction and enforcement provisions in the operative contract should be carefully considered and crafted.

Because seeking to enforce a foreign judgment in India can be arduous, time consuming, expensive, and unpredictable, it may actually be advisable for the US customer, depending on the circumstances, to institute claims initially in India against the Indian service provider with few meaningful assets in the US rather than pursuing a US judgment and still be faced with the necessity of effectively re-litigating the dispute in seeking to enforce the US judgment in India, particularly if the US plaintiff is seeking injunctive relief and time is of the essence. Therefore, jurisdiction and enforcement provisions in the operative contract should be carefully considered and crafted so as to provide the US customer with adequate and flexible rights and remedies keeping in view the nature of the business or knowledge process and the underlying customer IP being offshored to India.

To assess its likely ability to enforce rights and remedies with respect to an Indian service provider, the US customer should perform due diligence upfront to identify the physical location of the Indian service provider's assets. This exercise should include determining the extent to which the Indian service provider has a US presence and, correspondingly, local assets which would be available for the satisfaction of judgments. Furthermore, to mitigate any enforcement risks, the US customer should explore alternative measures such as insurance, performance bonding, letters of credit or guarantees from the Indian service provider and financially responsible affiliates of the Indian service provider, and retain for itself flexible and rules-based termination rights. To best mitigate the risk of an Indian service provider seeking refuge in an Indian court and being mired in prolonged litigation and subject to unfamiliar procedures, private arbitration is the preferred means of dispute resolution in an offshore sourcing transaction involving India.

CONSIDERING ALTERNATIVE DISPUTE RESOLUTION MECHANISMS TO MAINTAIN CONFIDENTIALITY

In India, litigation concerning the breach of trade secret protection clauses can lead to the open disclosure and consequential loss of the trade secrets at issue if the legal proceedings are not closed. Therefore, among other reasons, the operative contract should require that all disputes relating to the US customer's trade secrets and confidential information be subject to confidential mediation or arbitration rather than litigation and in a non-Indian venue if possible, and that all IP and information involved in the proceeding to be treated

confidentially. The relative ease of enforcing foreign and India-based arbitral awards in India further provide compelling reasons for adopting arbitration as the formal dispute resolution mechanism in India.

DETERMINING THE APPROPRIATE OFFSHORE DELIVERY MODEL

A potential US customer may consider adopting a “captive” offshoring model (which involves offshoring through affiliated legal entities in India) when the adverse impact and cost to the business of losing control over the IP that would be transferred to, or created in, India would be significant. Not surprisingly, a high percentage of captive offshoring transactions in India are in the IP-intensive sectors such as advanced software, high-tech electronics and pharmaceuticals. While establishing a captive in India provides the US customer more control over day-to-day operations and IP, a customer must balance that benefit against the fact that captive models tend to be more expensive and a majority of the legal issues discussed above will nonetheless still exist and therefore must be carefully evaluated and addressed irrespective of the offshore delivery model elected by the customer.

Conclusion

In summary, offshoring to India can not only yield enormous cost savings and increased efficiencies but also leverage India’s vast knowledge class to perform “high end” KPO services and functions. However, because of the potential risks to a customer’s IP that may be transferred to or created in India, a US customer contemplating an offshoring project in India must carefully assess India’s IP legal framework vis-à-vis the business or knowledge process that will be offshored and accordingly determine the necessary and available safeguards to protect its IP, including trade secrets and confidential information. These safeguards may include statutory and common law protections, but carefully crafted and robust contractual provisions combined with practical and enforceable mechanisms to minimize IP-related risk are mission critical and should be an integral component of any offshoring project in India. ♦