Knowledge Process Outsourcing to India: Important Considerations for U.S. Companies

Sonia Baldia
Doing Business in India:

Critical Legal Issues for U.S. Companies

Co-Chairs
Ashish S. Prasad
Mark L. Shwartz

To order this book, call (800) 260-4PLI or fax us at (800) 321-0093. Ask our Customer Service Department for PLI Order Number 11926, Dept. BAV5.

Practising Law Institute
810 Seventh Avenue
New York, New York 10019
KNOWLEDGE PROCESS
OUTSOURCING TO INDIA:
IMPORTANT CONSIDERATIONS
FOR U.S. COMPANIES

Sonia Baldia

*Mayer, Brown, Rowe & Maw LLP*

© Sonia Baldia 2006
Biographical Information

Sonia Baldia is a partner at the law firm Mayer, Brown, Rowe & Maw LLP. Her practice focuses on intellectual property procurement and management as well as information technology and business process outsourcing transactions, particularly involving India. Sonia is admitted to practice in New York and India only and is a Registered Patent Attorney at both the U.S. Patent and Trademark Office and at the Indian Patent Office. She can be reached at sbaldia@mayerbrownrowe.com
A new wave of global outsourcing to India known as knowledge process offshoring or "KPO" is following on the heels of the remarkably successful Indian market for information technology outsourcing ("ITO") and business process outsourcing ("BPO"). KPO involves the offshore outsourcing of knowledge-driven or "high end" processes that require specialized domain expertise, such 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. Unlike the ITO and BPO market sectors, which create cost savings solely through leveraging economies of scale and "rules based" process expertise, KPO accesses the global talent pool to carry out processes that demand specialized analytical and technical skills as well as the exercise of judgment and decision making. The strategic driver for KPO is to add value by providing high quality business expertise and superior productivity through improved time to market in addition to realizing the traditional cost reductions through arbitrage of labor markets that have made ITO and BPO successful.

Although there are vast first-mover benefits to U.S. and European KPO participants in KPO, notwithstanding those benefits meaningful challenges exist that must be addressed and navigated knowledgably so as to achieve and maximize the strategic incentives the KPO model offers. This article raises some of the key issues and risks that any potential KPO customer should carefully assess when considering KPO in India and analyzes more specifically two of the most critical issues associated with KPO to India—IP protection and data security. The article gives an overview of India's legal and IP and data security framework and enforcement mechanisms, identifies key risks for consideration, and recommends strategies to mitigate IP and data security risks in KPO transactions.

**ATTRACTION OF INDIA'S "KNOWLEDGE CLASS" FOR KPO AND FIRST MOVER ADVANTAGE**

The reward of successfully implemented KPO is truly enormous. The global KPO market is poised to grow over 45% per annum to $17 billion in 2010.\(^1\) India is emerging as the global KPO "hotspot" and is expected to capture over 70% of the market share going forward. India has a large reservoir of English speaking, knowledge-based professionals\(^2\) who are available at extremely competitive salaries and a rapidly evolving legal

---

1. Study conducted by Evaleserve in 2004.
and regulatory environment that is based on a western model and increas-
ingly friendly to foreign investment.

Unlike ITO and BPO, however, which are almost exclusively cost-
based and benefit from an almost unlimited relatively quickly trainable
labor pool in developing countries such as India and China, KPO depends
on a more limited, albeit currently vast, resource of highly-skilled, edu-
cated workers. These workers over time will almost certainly demand
more economically rewarding compensation packages as competition for
their skills increases. Successful KPO participants accordingly will not
only leverage existing resources but should also consider investing in, and
visibly participating in, education and training systems in an effort to
assure a predictable future supply of highly-skilled workers and to
develop branding of the company in Indian society, as many companies
(Microsoft, GE, and American Express, to name a few) already are doing.
Because of this timing consideration inherent in India’s increasingly
developing worker base first mover considerations are therefore not insig-
nificant with respect to KPO strategy.

The future prospects for KPO in India are immense because KPO is
applicable to multiple industry sectors in which India’s highly-skilled
workers and technically educated professionals have developed particu-
larized expertise. These sectors include finance, pharmaceuticals, health-
care, biotechnology, insurance, electronics, software, aerospace,
automotive, textiles, industrial machinery, entertainment, media and pub-
lishing, education, law, and engineering. A number of U.S. businesses
have already made successful forays into the KPO domain in India to
leverage what can be termed as India’s “knowledge class,” such as GE,
IBM, Microsoft, HP, Intel, Oracle, Cisco, Texas Instruments, Sun Micro-
systems, Philips, Motorola, JP Morgan, Citigroup, McKinsey, Goldman
Sachs, Reuters, Morgan Stanley, United Airlines, Ford, General Motors,
and Caterpillar, to name a few. Not only will many of these businesses
likely expand their KPO operations in India, but a whole host of new
entrants will assuredly also seek to leverage India’s growing KPO sector.

---
2. India produces 441,000 technical graduates, nearly 2.3 million other graduates
   and more than 300,000 postgraduates every year. A Survey of Business in India
3. A Deutsche Bank research report published in October 2005 reports that wages
   for skilled workers in India are rising on an average by 12-15% per year.
4. The National Association of Software and Service Companies (NASSCOM)
   predicts that the Indian IT sector faces a shortfall of 500,000 professionals by
   2010 that threatens India’s dominance of global offshore IT services. Financial
Two examples of KPO in India in key industries are worth noting. In the pharmaceutical industry, global pharmaceutical companies such as AstraZeneca, GlaxoSmithKline, Pfizer, Novartis and Eli Lilly, to name a few, have moved some portions of their clinical drug testing to India in an effort to tap into India’s vast and diverse population and pool of highly-skilled, but lower-wage demanding, scientists, which can significantly accelerate the trial time and time to market for new drugs on top of potential cost savings of up to 40-60%. India’s vibrant local pharmaceutical sector and its recently amended patent laws\(^5\) granting patent protection to drugs and chemical products on top of the process protection historically provided have also attracted global pharmaceutical companies to offshore R&D to India.

Investment incentive policies ranging from tax holidays to duty exemptions as well as India’s acceptance of the International Conference on Harmonization guidelines for Good Clinical Practices further enhance India’s attractiveness as an offshore destination for clinical research. With the cost of bringing a new drug to market continuing to increase in the U.S., with the latest estimates approaching US$1 billion,\(^6\) the possibility of potentially reducing the cost of clinical trials and drug discovery by up to 50% by moving those processes offshore cannot be ignored. Increasing pressure on pharmaceutical companies to improve productivity and profitability without sacrificing quality to sustain competitive advantage makes KPO a compelling strategic route.

Similarly, the financial services sector has experienced tremendous growth in India, with leading global financial institutions (such as JP Morgan, Citigroup, Prudential, Goldman Sachs and ABN Amro) offshoring high-end work to India either through delivery by affiliated legal entities in India or by unaffiliated pure-play third party vendors. Most of these businesses originally outsourced IT-enabled common finance and accounting processes that are transactional in nature, such as accounts payable, accounts receivables and payroll, but have gradually migrated to offshoring high-end financial processes, such as equity research, business intelligence, credit risk analysis, insurance claims processing, to name a few.

**KPO DELIVERY**
When it comes to the KPO delivery model, one size does not fit all. Currently three key KPO delivery models exist, which are (i) offshoring

---

through affiliated legal entities in India, which can be thought of as “Captive KPO,” (ii) contracting with unaffiliated third party vendors, or what can be called “Third Party KPO,” and (iii) partnering with local entities to share control of local operations used for delivery of KPO services, or “Joint Venture KPO.” Each model has its own advantages and risks, and should be evaluated carefully so as to identify and assess the relative pros and cons for a particular KPO strategy. Businesses should adopt different delivery models taking into account numerous variables, including the nature and scope of the activities to be offshored, previous offshoring experience, concerns about security and control of IP, risk tolerance, tax considerations and budgetary constraints.

For example, Third Party KPO can be more quickly implemented and often can offer greater flexibility in access to talent, scalability and cost structure. But it also yields to the third party more control over day-to-day operations and the handling of sensitive data and IP, and creates more reliance on the foreign host country’s legal regime and the timely enforcement of contracts. In comparison, a Captive KPO model usually requires more time to implement and provides less flexibility to ramp up or down quickly, but it ensures substantially more control over the management of the offshore operations and the company’s sensitive data and IP, and less dependence on foreign enforcement of contract rights. A KPO customer should consider adopting the Captive KPO strategy if the scope of KPO involves a substantial transfer to India of the customer’s critical proprietary technology, IP, or data and the enterprise cost of possibly losing control over some meaningful component of any of those assets is high. In India, KPO initially took hold in captive centers through the establishment of local subsidiaries and reportedly over 50% of offshore business in India is currently Captive KPO. But as the Indian KPO market matures and the business, legal and regulatory environment there continues to advance and stabilize, businesses can be expected to increasingly leverage the Third Party KPO model in light of the advantages that model offers in terms of flexibility, scalability, and range of expertise.

Regardless of the delivery model, KPO invariably requires the customer to disclose and share knowledge-intensive processes with the offshore provider, which knowledge may be in the form of proprietary technology, software, chemical entities, specifications, product designs, business processes, methodologies, drug formulations or other sensitive data. Accordingly, the substantial benefits that KPO in India offers must be seen as “hand in hand” with the unique and heightened risks inherent in the transfer of customer-owned knowledge to India. As discussed
below, these risks must be carefully considered upfront and mitigated to realize the full benefit of KPO to India.

OVERVIEW OF INDIA
KPO by definition involves a deeper investment by the customer in the host country’s educated workforce and a dependence on that workforce that far exceeds BPO and ITO, and a greater dependence on the stability and predictability of the underlying governmental and social structure of the host country. As a result, a deeper understanding of the host country’s political and legal framework is useful.

India's Political and Legal Systems
India is the largest democracy in the world. India today is a union of 25 states and 7 self-governing territories established under the country's 1950 constitution. India gained independence from British colonial rule in 1947. The adoption of the constitution on January 26, 1950, did not disturb, however, the existing laws or court system established under colonial rule. India has a parliamentary form of government patterned after Britain's parliament and its legal system is also patterned after Britain's judiciary.

India’s president is the constitutional head of the government’s executive branch. Executive power, however, resides in the Council of Ministers, known as the Cabinet, which is led by the Prime Minister. The power to amend the constitution resides in the two houses of parliament. India’s constitution governs the sharing of legislative power between parliament and India’s 25 state legislatures. The Parliament has exclusive jurisdiction over matters of national interest, as enumerated in what is known as the Union List. This list includes defense, foreign affairs, currency, income tax, railways, shipping, posts and telegraphs. State legislatures have exclusive jurisdiction to legislate with respect to matters enumerated in what is known as the State List, which includes public order, police powers, public health, communications, and education. Other policy areas also exist over which parliament and the state legislatures have concurrent legislative interest and powers, and these matters are found in the Concurrent List. This list includes criminal law, marriage and divorce, trade unions, and price controls. Local governments in India have far less autonomy.

India’s independent judicial system began under colonial rule and still closely resembles British common law courts in terms of both civil and criminal procedures and the use of decisional case law and the application
of, and reliance on, case precedent, or *stare decisis*. Directly subject to the review of India’s highest court, the Supreme Court, are 18 intermediate appellate courts or High Courts, with one High Court presiding over either one state or a group of states. Under each of the High Courts exists a hierarchy of courts of general jurisdiction. India’s law is based on the Constitution, statutes, governmental regulations, and case law. Of course, state and local governments also promulgate state statutes and local ordinances, but these are in many cases subject to pre-emption by acts of parliament. Although India has over 25 national languages, including the widely-spoken Hindi as India’s official language, English is the common working language in the public and the private sectors in India’s metropolitan areas. All official publications are available in English.

**India’s Legal and Economic Strides Toward Modernization**

For almost four decades after it gained independence in 1947, India was known as a “closed economy,” substantially restricting and controlling all forms of foreign investment or technical collaboration in India. India operated on an economic policy of import substitution and technological self-reliance (*swadeshi*), making the business climate significantly less conducive to foreign investors. Until the late 1980s, a complex and highly bureaucratic regulatory framework controlled the flow of international capital and technology to local markets. In the late 1980s, however, liberalization efforts began and in 1991 those efforts culminated in watershed reforms. Beginning in 1991, India substantially liberalised its regulatory regime through reforms to its industrial policy and by making the investment climate more conducive to foreign investment and technology transfer. The basic thrust of the new policies has been to move from a highly regulated to a market driven system.

As a result, India today enjoys a vastly different, progressive commercial climate, with a robust and mixed economy in which the private sector plays an increasingly prominent role in the country’s economic development and the attraction of foreign capital. Since 1991, technology inflow and foreign investment have dramatically increased in India. Today, India has the fourth largest economy in the world, the second largest population in the world, the second largest gross domestic product among developing countries based on purchasing power, and a large and growing market at an estimated 8% per annum. In addition, India has the second largest pool of English speaking skilled workers in the world and is globally recognized for high-value add, low cost work. These factors, coupled with strategic investment incentives and an increasingly dependable and
modernized legal system and capital markets, have served as a catalyst for India to become the most preferred offshore location in the world.

INTELLECTUAL PROPERTY AND KPO

Protection of IP is a critical concern in every KPO. It is a legal concern and a strategic business issue because IP assets are mission critical in today's knowledge-based economy. A KPO often involves sharing, or the creation of, multiple types of IP rights (such as trade secrets, trademarks, industrial designs, patents, copyright, mask works, etc.), each of which is governed by its own distinct national law. Such IP rights can be further categorized depending on how the IP is shared or created, such as customer IP versus service provider IP, and this can be further sub-categorized into new or pre-existing IP. IP ownership, infringement, and piracy are the most critical concerns that must be thoroughly and carefully addressed in every KPO, including any KPO to India.

IP issues are compounded in a global KPO in which a U.S. customer's IP will be shared or created across multiple jurisdictions. Regardless of the KPO delivery model employed, a U.S. customer must often necessarily make its IP—ranging from proprietary designs to business processes to chemical formulae—available to the Indian service provider (which may be a third party vendor, a business partner or local workforce at a corporate affiliate) so that the offshored functions can be performed effectively. In addition, new IP might be created by the Indian service provider on behalf of the U.S. customer. This sharing and creation of IP across multiple jurisdictions creates for the U.S. customer very real potential vulnerabilities because of the "territorial" or "national" legal nature of IP rights, meaning that the host country's IP laws may control IP-related disputes adjudicated in that country. In other words, U.S. IP laws may not, and likely will not, be applied in the host country regarding IP ownership disputes even if the operative contract between the U.S. customer and the offshore service provider has an unambiguous governing law provision calling for a specific U.S. state's laws or U.S. federal law to govern.

Further complicating this issue, it is also the case that a U.S. court may not apply U.S. IP laws, but rather foreign IP law, to decide issues involving the ownership of IP created abroad notwithstanding the operative contract's governing law and venue provisions. In 1998, in a case titled Itar-Tass Russian News Agency vs. Russian Kurier7 involving copyrighted work created in Russia, the U.S. Court of Appeals for the Second Circuit applied the "work made for hire" doctrine under Russian law to determine

the initial ownership of the copyright of the works in suit. This decision has significant implications for a U.S. customer contemplating a KPO transaction that involves the creation of IP in India because this significant U.S. court's analysis suggests that Indian IP law could determine ownership in a disputed copyright work created in India notwithstanding the operative contract’s adoption of U.S.-based governing law.

Since IP protection and enforcement mechanisms for IP rights (e.g., patent, trademark, trade secret, copyright, and mask works, to name several) are not harmonized around the world, they differ in material respects on a country-by-country basis. This can affect a U.S. customer's expectations in the offshoring arrangement and, in the absence of appropriate contractual safeguards, can potentially jeopardize a U.S. customer’s rights to its own IP or critical third party technology. Therefore, in any KPO a U.S. customer must (i) thoroughly and carefully perform legal due diligence on national and local IP laws and customs, (ii) assess the possible impact on the contemplated KPO transaction, and (iii) structure measures that will adequately protect against the potential risk of losing control of IP so that the purpose of the KPO may be successfully accomplished.

INDIA’S IP LEGAL FRAMEWORK AND ENFORCEMENT

Framework Overview

While India is perceived as providing better IP protection compared to a majority of the other offshore jurisdictions, such as China, Russia and Mexico, India’s IP laws and enforcement mechanisms are nevertheless weak compared to western IP laws and practices, such as in the U.S. and in Europe. India, however, is a member of the World Trade Organization (“WTO”) and generally complies with the minimum standards stipulated by the WTO Agreement on Trade Related Aspects of Intellectual Property Rights. India also is a signatory to major international IP harmonization conventions, such as the WIPO treaties, which include Universal Copyright Convention, Berne and Paris Conventions and the Patent Cooperation Treaty.

India also provides express statutory protection for patents,8 copyright,9 trademarks,10 designs11 and mask works.12 Most recently, India amended its patent statute finally to provide for statutory patents for

drugs, chemicals and agricultural products in addition to the historically available patent protection for process of manufacture.\textsuperscript{13} India has made substantial improvements to its IP regime in the last decade to foster innovation as well as to attract foreign investment. Despite these measures, however, some gaps remain in India’s IP regime and the actual implementation and enforcement of IP rights remains weak and ineffective in comparison to U.S. standards.

**Enforcement Overview**

In India, the enforcement system for IP rights includes civil remedies as well as criminal penalties. Most disputes in India relating to IP infringement settle out of court without trial. Civil cases historically require years to come to trial and a criminal case can similarly require a number of years before it is finally concluded in India’s court system. Another discouraging factor for IP owners in pursuing civil claims in India is the difficulty in proving the actual extent of damage caused by the infringement and in recovering reasonable compensation. Typically, the monetary damages awarded by Indian courts are meagre compared to U.S. awards. Indian IP law only provides for compensatory damages based on the principle of restitution of the loss actually suffered. No statutorily trebled damages or punitive damages are available for example, which particularly creates a less than optimal deterrent against piracy. While Indian IP law does not impose copyright or trademark registration requirements as a prerequisite to enforcement, registrations still serve a very important evidentiary function because they are deemed prima facie evidence of validity and trigger statutory damages in infringement suits.

Recent amendments to Indian civil procedure code as well as more recently issued judicial precedents, however, signal an improvement in the enforcement area. In 2002, India amended its code of civil procedure to impose mandatory time limits and associated penalties on the litigants at each stage of the litigation to reduce delays in the civil litigation process in India.\textsuperscript{14} While these new and ambitious requirements may likely


\textsuperscript{13} The Patents (Amendment) Act, 2005.

\textsuperscript{14} The Code of Civil Procedure (Amendment) Act, 2002.
be honoured more in the breach, it probably will cause a more expeditious disposition of civil cases in Indian courts. Also, in 2005 the Delhi High Court opened the door for awarding punitive damages for the first time in a copyright infringement case, observing that the level of punitive damages should be commensurate with the degree of the infringing misconduct.\footnote{Microsoft Corporation v Deepak Raval & Anr, 2005 (33) PTC 122 (Del.); Time Incorporated v Lokesh Srivastava, 2005 (30) PTC 3 (Del.).}

Despite improvements, civil litigation in India remains a relatively marginal enforcement tool and foreign IP owners engaged in KPO there should plan to rely instead on thorough and carefully negotiated contracts that are based as much as possible on rules-based performance rather than standards-based conduct. For example, rules-based service level criteria (the well-known “five nines” criteria, for example) can be objectively measured, verified and monitored and present far less room for contestable dispute and hence should be always sought where possible over standards-based benchmarks such as “reasonable” or “best” efforts, for example. Efforts should also be made in contract negotiations to create a clear basis for seeking to have disputes resolved in preferable offshore venues where stronger remedies that better protect the IP may exist, whether in U.S. or European courts or arbitrations. But a KPO customer in India cannot count on the enforcement of such venue obligations if challenged in an Indian venue regardless of the contract and therefore must create as “airtight” as possible contract with respect to the underlying substantive obligations so that Indian-based adjudicative bodies, whether courts or Indian appointed arbitrators, have objective and verifiable evidence and data to evaluate and decide upon and need only apply minimal subjective analysis.

The most effective remedy in India to block and deter IP infringement is injunctive relief with respect to the enforcement of statutory IP rights. Injunctive relief in response to breach of contract claims is available but less easily obtained. Other remedies, such as \textit{ex parte} search warrants and seizure orders, known as an Anton Pillar Order,\footnote{This order derives its name from the British case \textit{Anton Piller KG v. Manufacturing Processes Ltd.}, 1976 (1) All. E.R. 779, and is a pre-emptive \textit{ex parte} injunction that aims at protecting the plaintiff against the activities of an unscrupulous defendant, who may destroy or remove incriminating evidence.} can also be obtained in civil actions. In India, criminal prosecution is available only in trademark and copyright cases, but not in cases involving patents or designs. More specifically, criminal remedies are available against any person who
knowingly infringes or abets the infringement of a copyright or who uses or applies false trademarks and trade descriptions with the intent to defraud. Few criminal prosecutions relating to IP misconduct have emerged from Indian courts to date, but there are promising signs that Indian criminal law might become a more realistic deterrent.

Because of the weaker enforcement of India's IP laws, counterfeiting and piracy continue to be rampant in India and accordingly a serious problem for U.S. companies doing business there. It presents serious challenges to the Indian government in promoting India as a destination for innovation and high-end technology development. In 2004, U.S. companies lost over $500 million in sales due to piracy in India of copyrighted works, particularly software, sound recordings, films, popular fiction and other books. For these reasons, in the last several years the U.S. Trade Representative has placed India on the "Priority Watch List" as part of what is known as the Special 301 review, which identifies foreign countries that deny adequate and effective protection of IP rights and is one of the trade measures adopted by the U.S. to exert pressure on India to strengthen its IP laws and enforcement.

From the KPO perspective, one of the most troubling gaps in India's IP legal framework is that India does not provide any statutory protection for trade secrets or confidential information. The U.S. provides statutory protection to trade secrets, both at the state and federal level, with meaningful civil and criminal remedies to counter misappropriation of trade secrets, including actual and punitive damages, injunctions, attorneys' fees, but that is not the case in India.

PROTECTING TRADE SECRETS AND CONFIDENTIAL INFORMATION IN INDIA

In a KPO, a primary concern should be the Indian service provider's ability to safeguard trade secrets and confidential information of commercial value against misappropriation, misuse, unauthorized disclosure, sabotage or theft. Most of the knowledge shared in an offshore KPO transaction (for example, source code, formulae, designs, specifications, and experimental data) is confidential in nature and not suitable for local registrations in the form of patents. It therefore becomes critical for the KPO

---

17. 2005 United States Trade Representative Special 301 Report available at www.ustr.gov
18. 2006 United States Trade Representative Special 301 Report available at www.ustr.gov
customer to give serious thought as to how it will best protect this information to maintain the company’s competitive advantage.

Because no statutory protection is afforded to trade secrets in India, parties mainly rely on contract to protect trade secrets. In addition to contractual obligations, Indian common law also recognizes the common law tort of “breach of confidence” irrespective of the existence of a contract. But the tort’s utility is limited in a KPO context because the duty of confidence at issue can be enforced only against a party that is either a fiduciary or in an employer-employee relationship with the complaining party. Also, arguably the duty only prevents the unauthorized disclosure of confidential information to a third party and does not prevent the recipient’s own “misappropriation” of the information.

Consider the following hypothetical involving an Indian KPO service provider that has engaged a subcontractor in India to perform KPO services for a U.S. customer. If the Indian subcontractor discloses or misappropriates the U.S. customer’s trade secrets or confidential information, the U.S. customer has no breach of confidence claim against the subcontractor and, unless the U.S. customer has contracted directly with the subcontractor, has no breach of contract claim either. The contract between the U.S. customer and the Indian KPO service provider may also hold the service provider liable for damages caused by the subcontractor’s disclosure, but that cause of action still does not directly address or foreclose the subcontractor’s past and future misconduct. Essentially, the U.S. customer is left without a direct remedy against the Indian subcontractor.

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 U.S. client of the person’s ex-


20. Under a pending new bill that proposes to amend India’s Information Technology Act, 2000, a general supplier will not be liable for subcontractor misconduct unless the general supplier was itself negligent in some way.
employer, to the U.S. 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 U.S. 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 U.S. 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 U.S. 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 both 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 and the Indian government is responding. While that is encouraging, the perils of subcontractor and employee misconduct as to IP in India remain very real, and it is therefore critical for U.S. customers to be aware of this enforcement gap and address it in the operative KPO contract with the Indian service provider and in the contracts between the Indian service provider and its subcontractors to create as best as possible an enforceable contract right for wrongful disclosure and misappropriation directly among the customer and the service provider and the subcontractor.

**Recommended Practices to Safeguard Trade Secrets and Confidential Information**

Based on the foregoing discussion, trade secrets and confidential information must be protected through the contractual arrangement between the U.S. 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 U.S. customer against the subcontractors.

Confidentiality and non-competition covenants are enforceable under Indian law. To date, this is the only reliably effective way to protect trade secrets and confidential information in India. A U.S. customer must therefore insist upon unambiguous provisions in the operative KPO 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.

In addition, prior to entering into the final contractual arrangement, the U.S. customer should perform as thorough as possible due diligence to make sure that the Indian service provider has written employment and non-disclosure agreements in place with its employees and consultants and closely scrutinize such agreements to make sure they are sufficiently protective of the U.S. customer’s rights and interests and are valid and enforceable under Indian law. To the extent practicable, a U.S. customer should consider entering into non-disclosure agreements directly with the Indian service provider’s employees and consultants assigned to the project. This way the confidentiality obligations will remain in force even after the employee or consultant is no longer employed or engaged by the Indian service provider and the U.S. 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.

The operative KPO 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 U.S. 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 the precise terms cannot be assumed to be enforceable. More specifically, the Indian Contract Act stipulates that an agreement will not be enforced to the extent that it restrains a person from exercising a lawful profession, trade or business.21 However, judicial precedent indicates that an Indian court will enforce a restrictive covenant if it meets the “reason-

ablleness” 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.*[^22^], 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,[^23^] thus making the drafting of these provisions in KPO contracts a critical and sensitive task.

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 KPO services and to the extent possible the U.S. customer should require that subcontractors enter into contractual commitments that are directly enforceable by the U.S. customer. At the very least, the U.S. 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 U.S. 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) provide for the ability of the US customer to directly enforce data privacy, confidentiality and IP ownership provisions against the subcontractor.

In addition, effective information governance strategies and internal security measures should be implemented 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 U.S. 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

[^22^]: AIR (1967 SC 1098).
and conducting exit interviews for ex-employees to remind them of continuing confidentiality obligations, (v) performing routine audits to verify 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.

Finally, discussed further below in connection with dispute resolution generally but worth noting here, in India trade secret litigation may lead to the loss of trade secrets at issue since legal proceedings may not be held in secret. Therefore, the operative KPO contract should require that all disputes relating to the U.S. customer's trade secrets and confidential information be subject to mediation or arbitration rather than litigation and in a non-Indian venue if possible.

NAVIGATING INDIA'S LANDSCAPE OF OTHER IP LEGAL DOCTRINES

While India's IP laws are rooted in common law as in the U.S. and Britain, and even though Indian courts often consider British and U.S. legal precedent in decision making, many differences exist in the respective IP laws of these countries. These differences can sometimes be quite subtle and thus catch a U.S. customer off guard and potentially undermine its IP rights unless it has previously addressed these less obvious gaps in India's IP protection through alternative mechanisms. Addressed summarily below, as examples, are the "work made for hire" doctrine, the "joint ownership" rules, the "fair use" exceptions, and the "inalienable rights" doctrine.

Work Made for Hire

The "work made for hire" doctrine is an important protection in the U.S. governing copyright ownership in deliverables and it extends to inventions created by employees as well as independent contractors. Indian copyright law recognizes this doctrine, but it is not as well developed as in the U.S. and therefore not a fully reliable safeguard in those circumstances in which IP will be developed in India. Under Indian law, this doctrine only extends to employee-created inventions and does not apply with respect to contractor-created inventions. Consequently, unless the contractor-created inventions are expressly assigned by written contract to the U.S. customer, which is permitted under Indian IP law, the legal owner of the inventions under Indian law will be the contractor that developed them.

24. Section 17 of the Copyright Act, 1957.
Therefore, the operative KPO contract with the Indian service provider (irrespective of whether it is a wholly-owned subsidiary in a Captive KPO model or a third party vendor in a Third Party KPO model) must include valid assignment provisions transferring the copyright to the US customer and these provisions should flow down into agreements with the Indian service provider’s employees and subcontractors. As the determination of ownership rights in IP created in India may hinge on Indian IP laws, employment and contractor agreements should be carefully scrutinized to make sure that the ownership rights are appropriately assigned and are valid and enforceable under Indian law. Absent a transfer of full legal title or an exclusive license under the relevant copyright, a U.S. customer may not have standing to sue in the U.S. or India for infringement.

Finally, because each additional tier of relationships potentially complicates the U.S. customer’s management of IP ownership and the chain of title to the IP, the U.S. customer’s general and precautionary approach should be to avoid involving offshore subcontractors, to the extent practicable, in development projects.

**Inalienable Rights**

Another point of departure between the U.S. and Indian copyright laws is that in India certain inalienable "moral rights" attach to authors of copyright work allowing them to restrain or claim damages for the distortion or modification of work if it could bring them “disrepute.” 25 These rights are retained by the authors even if the copyright work is assigned but such rights may be waived under limited circumstances. 26

A U.S. customer should therefore seek a waiver of such moral rights by the author upon assignment of all copyrighted materials. Without a waiver of such rights, the assigning author will likely be able to restrain future versions of copyrighted materials, particularly if the author believes such versions may contain defects or errors that might bring the author disrepute. It is worth noting, however, that moral rights do not apply with respect to computer software in India. Accordingly, absent agreement to the contrary, an author may not object to the modification of a software work by a U.S. customer who has acquired the right to adapt the work.

---

25. Section 57 of the Copyright Act, 1957.
26. *Amar Nath Sehgal v Union of India & Anr*, 2005 (30) PTC 253. In this case, the Delhi High Court upheld the plaintiff’s moral rights in the copyrighted work (murals) created by the plaintiff even though the work was assigned to, and owned by, the defendant.
**Fair Use Exceptions**

Under Indian copyright law, certain uses of computer programs without the copyright owner’s permission, including “non-commercial personal use,” are deemed “fair use” and do not constitute infringement. Furthermore, Indian copyright law does not require that any payment be made to the copyright owner for such use. These so-called “fair use exceptions” reflect the historic emphasis of Indian law on public access to knowledge. This fair use doctrine has been subject to very limited judicial scrutiny in India and is unfortunately a murky legal concept that leaves a blurred line between lawful and unlawful use. India’s fair use exceptions significantly exceed those in the U.S., which only permit copying or use of limited portions of copyrighted works without the owner’s consent for limited purposes of commentary, criticism, teaching, and research, and similar specific activities.

As a result, the operative KPO contract must strictly prohibit any use, copying, reverse engineering or distribution of the U.S. customer software code beyond the purposes expressly authorized by the U.S. customer. Having said that, it is unclear however if these contractual protections will override the statutory provision permitting “fair use” under India’s copyright law because there is no case law on point to date. India’s “fair use” law has been subject to intense scrutiny and push back from the U.S. software industry. There is currently significant pressure on India to narrow these exceptions and reform its copyright laws to align with international practices.

**Presumptions in IP Licenses and Assignments**

Under Indian copyright law, certain presumptions apply to licensing and assignment of copyrights, which if not adequately addressed through contractual mechanisms can jeopardize the U.S. customer’s rights in IP created in India or licensed from the Indian service provider. For example, Indian copyright law provides that unless a copyright license or assignment expressly states that license or assignment rights are worldwide and perpetual, the license or assignment rights are limited to India and for a period of 5 years only from the date of the license or assignment, as applicable. Similarly, unless a copyright assignment expressly states other-

---

27. Section 52 of the Copyright Act, 1957.
28. *Gramaphone Co. of India v Mars Recording Pvt. Ltd.*, 2000 PTC 117 (Kar). In this case, the Karnataka High Court justified the statutory “fair use” provisions as balance between the rights of authors and interests of society.
29. Sections 19 and 30A of the Copyright Act, 1957.
wise, the assignment lapses if the assignee has not "exercised" its rights within one year from the date of assignment.\textsuperscript{30} Under Indian patent law, a patent assignment must be in writing and registered in India otherwise it is invalid.\textsuperscript{31} These are all important considerations because Indian law may be used to determine IP ownership and infringement issues that arise with respect to IP transferred to, created in, or licensed from, India even if the operative contract calls for non-Indian law to apply.

**Joint Ownership Rules**

KPO projects can involve collaborative efforts that then raise issues concerning whether IP generated from those efforts is, or should be, jointly owned and whether joint ownership is a preferable or desirable arrangement. Joint ownership of IP in any jurisdiction is fraught with land mines and as a rule of thumb should be avoided to the extent possible, and in India becomes even more risky and legally opaque.

Unless the parties contractually and unambiguously define in detail the treatment of jointly owned IP and the joint owners' respective rights therein at the outset of the transaction, joint ownership will cause problems and conflicts. Further complicating the issue, rules governing joint ownership of IP vary by type of IP right and by country and therefore can affect a U.S. customer's expectations in the KPO transaction. For example, under U.S. law, joint ownership in a patent means that each joint owner owns and controls a 100% interest in the patent, just like joint tenancy with respect to real property, and can exploit the patent without the consent of, or any accountability to, the other joint owner. In the case of copyrights, however, in the U.S. a joint owner of a copyright must obtain consent of the other co-owners prior to commercially exploiting the jointly owned copyrighted work. This can create particular uncertainty with respect to software-related IP, which is protected both by patent and copyright. In India, a joint owner of a patent cannot commercially exploit the patent without obtaining consent from the co-owner and must also provide an accounting to the co-owner in connection with any license, assignment, or sale of the patent.\textsuperscript{32} Because there is no statutory reasonableness standard with respect to the withholding of consent by a joint owner, the U.S. customer is subject to the whims of a joint owner if the U.S. customer wishes to exploit a jointly owned patent in India. In this circumstance, limited recourse may however be available by making an

\begin{itemize}
\item \textsuperscript{30} Section 19 of the Copyright Act, 1957.
\item \textsuperscript{31} Section 68 of the Patents Act, 1970.
\item \textsuperscript{32} Section 50 of the Patents Act, 1970.
\end{itemize}
application to the Controller of Patents who has the statutory power to
direct certain actions of joint owners.\textsuperscript{33} Furthermore, joint ownership of a
patent or copyright can also affect a joint owner's ability to enforce its
rights in the patent or copyright against a third party because Indian law
requires all owners of a patent or a copyright to be parties in an infringe-
ment lawsuit.\textsuperscript{34}

Additional issues to consider, which are gray areas under Indian law,
are a joint owner's responsibilities relating to filing, prosecution, mainte-
nance and enforcement of IP rights in jointly owned inventions in the
applicable jurisdictions. Therefore, if and to the extent joint ownership of
IP is contemplated in the KPO transaction, the operative contract must
clearly define each joint owner's responsibility for (i) determining which
inventions will lead to the filing for statutory protection and in which
countries these filings will be made, (ii) obtaining any applicable foreign
filing licenses and prosecuting the filings, and (iii) on-going use, mainte-
nance and potential enforcement and licensing of any issued statutory IP
rights. For the foregoing reasons, careful consideration should be given to
IP that may flow from the results of joint work.

\textbf{DETERMINING LOCAL PATENT STRATEGY}

Before embarking on a KPO to India, a U.S. customer should determine
its patent strategy with respect to its patents or patentable inventions that
might be shared or created in India. A fundamental question should be
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 as well as any subsequent global
filings for any India-originated innovation. Through a well thought out
patent strategy upfront, a U.S. customer can minimize not only infringe-
ment risk but also the risk of potential loss of any global patent rights, par-
ticularly given the differing standards of patentability worldwide.

For example, the standards of patentability under U.S. patent law (such
as for claiming priority, disclosure requirements during prosecution of the
patent application, and interference practice, to name a few) significantly
differ from those under Indian patent law. In contrast to the U.S. first-to-
invent patent system, India has a first-to-file patent system and therefore
India does not provide for an interference process to determine priority of
invention if contested. On the other hand, the detailed interference pro-
ceedings in the U.S. permit a subsequent applicant to still obtain patent

\textsuperscript{33} Section 51 of the Patents Act, 1970.
\textsuperscript{34} Section 61 of the Copyright Act, 1957.
rights through documentary proof of earlier conception and diligent reduction to practice. If the Indian provider is unfamiliar with the U.S. patentability standards, which have little relevance to the Indian patent system, and as a consequence the service provider fails to maintain documentary proof of innovations in accordance with the U.S. evidentiary standards, this can potentially jeopardize a U.S. customer's ability to obtain and enforce patent rights in the U.S.

Therefore, it is critical for the operative KPO contract to (i) clearly define procedures for maintaining documentation of innovations that would serve as proper evidence of time of conception and reduction to practice so as protect the U.S. customer's right to seek possible U.S. patent rights and (ii) provide for periodic training as well as routine audits to make sure that the Indian service provider is in compliance with item (i).

To a large extent, the patent strategy will be driven by the nature of the KPO and the degree of critical IP involved. For example, in a KPO in India involving R&D 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, a U.S. customer may want 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 a bundle of strong statutory rights to the patent owner that may be enforced against any third party in India to stop it from any unauthorized use or infringement 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 U.S. KPO 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.\textsuperscript{35} India's patent laws also provide for "research and experimental use" exceptions, whereby a third party's experimental use of a patent, even if such use is for commercial purposes, without the patent owner's consent will not constitute infringement.\textsuperscript{36}

\textsuperscript{35} Section 84 of the Patents Act, 1970. Under this section, a third party may make an application for a compulsory license on the grounds that the "reasonable requirements of the public" have not been satisfied, or that the patented product is not available at a "reasonably affordable price," or that the patented invention is "not worked in the territory of India."
Indian patent law requires that applications for patents for inventions originating in India or involving an Indian resident inventor must first be filed in India, absent a grant of a "foreign filing license" by the Indian Patent Office.\textsuperscript{37} It is also noteworthy that India recently amended its patent laws to provide for patents for drugs and chemical products as well as software-related inventions, but it is not clear at this time how these new laws will be applied. Computer programs and business methods continue to be \textit{per se} not patentable in India, however, and so must be protected as trade secrets through the approaches discussed above.

\textbf{OTHER IP CONSIDERATIONS}

As a practical way to manage the risk to IP, the U.S. 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 U.S., 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 resources would be required to manage and integrate results from the various entities.

A potential KPO customer should seriously consider adopting a Captive KPO model when the cost of losing control over the IP that would be transferred to, or created in, India is high. Not surprisingly, a high percentage of Captive KPO transactions in India are in the IP-intensive sectors such as advanced software, high-tech electronics and pharmaceuticals. While establishing a Captive KPO in India provides the U.S. customer more control over day-to-day operations and IP, a majority of the legal issues discussed above will nonetheless still exist and therefore must be carefully evaluated and addressed irrespective of the KPO delivery model elected by the customer.

In light of the discussion above, a U.S. customer contemplating a KPO in India must carefully assess India’s IP legal framework vis-à-vis the knowledge process that will be offshored and accordingly determine the appropriate safeguards to protect its IP in India. These safeguards may be

\begin{footnotesize}

\textsuperscript{36.} Section 47 of the Patents Act, 1970.

\textsuperscript{37.} Section 8 of the Patents Act, 1970.

\end{footnotesize}
a combination of statutory, contractual and practical mechanisms to minimize IP-related risk. The KPO parties should clearly address in the contract, among other things, (i) the specific allocation of relative ownership and access rights to IP between the customer and the service provider not only for the duration of the transaction but also after the relationship is terminated, (ii) all desired non-disclosure and non-compete obligations of the service provider, (iii) any measures that the service provider will be required to implement to minimize risk to the customer’s IP, and (iv) all rights and remedies available to the customer to enforce its rights and protect against infringement or misuse of the U.S. customer’s IP, including immediate termination rights and uncapped liability for service provider misconduct.

Another important consideration is whether the customer IP being offshored to India (such as encrypted technology or source code) is subject to U.S. export controls, in which case a license to “export” or other approvals may be required from U.S. governmental agencies prior to offshoring the IP.38 Because the customer bears the responsibility for compliance with U.S. export control laws on behalf of itself and the offshored provider at the risk of severe civil and criminal penalties, the operative KPO contract should unambiguously require the Indian service provider to comply with, and facilitate the customer’s compliance with, applicable U.S. export control laws and the service provider’s failure to so comply should not only permit the customer to immediately terminate the contract but also result in uncapped financial consequences to the service provider. Another often overlooked, but important, issue which should be addressed upfront is whether any technology licensed by the U.S. customer from third parties will need to be transferred to the Indian service provider and, if so, whether the underlying licenses already permit such transfer or will require third party consents to permit it, which can add additional complexity and costs to the transaction.

DATA SECURITY AND PRIVACY CONSIDERATIONS
Along with IP, data security and privacy are also among the top concerns for a U.S. customer offshoring to India. A KPO routinely involves the

38. The three U.S. federal regulations that govern the “export” or “re-export” of certain US originated technology, equipment, software or information for reasons of national security are: International Traffic in Arms Regulations of the U.S. Department of State, 22 C.F.R. 120-130 (ITAR); Export Administration Regulations of the U.S. Department of Commerce, 15 C.F.R. 730-774 (EAR); and Office of Foreign Assets Control Regulations of the U.S. Department of Treasury, 31 C.F.R. 500 (OFAC).
transfer of sensitive personal data between the U.S. customer and the Indian service provider. Depending on the nature of the KPO to India, the Indian service provider may have access to a U.S. customer's confidential data, which may include personal information of its employees, customers or other third parties. For example, in a KPO involving medical transcription, credit card processing, preparation of tax returns, insurance claims or mortgage application processing, the Indian service provider will have access to personal information such as medical files, credit card information, social security numbers, dates of birth, and drivers' license information, that have the potential for misuse. Furthermore, connectivity networks between offshore service delivery centers and customer systems can create potential vulnerabilities for unauthorized access, viruses, and intrusions by hackers, for instance. Therefore, a critical concern for a U.S. customer is how to minimize the risk of unauthorized access to sensitive data and ensure that the Indian service provider meets privacy compliance requirements applicable to the U.S. customer.

**U.S. Approach to Data Privacy**

In the U.S., businesses are under increasing pressure through industry-specific federal and state laws and regulations to protect the personal data of their customers. For example, the Gramm-Leach Bliley Act of 199939 ("GLBA") protects the personal financial information of consumers held by financial institutions, which not only include banks, securities firms, mortgage brokers and insurance companies, but also companies providing many other types of financial products and services to consumers as well as other companies, whether or not they are financial institutions, who receive such information. The GLBA requires financial institutions to, among other things, (i) design, implement and maintain robust security measures to safeguard consumers’ personal financial data, (ii) make full disclosure of their privacy policies to consumers and provide "opt-out rights," and (iii) monitor the activities of any third party in the U.S. or overseas to which it transfers such data. Similarly, California recently enacted a law that requires businesses to notify California residents of any breach in the security of their personal data by unauthorized users.40 Similar laws requiring mandatory breach notification have been enacted by over 30 other states in the U.S.41 The Health Insurance Portability and

Accountability Act of 1996, commonly referred to as HIPPA, protects personal health and medical data of healthcare consumers. The Sarbanes-Oxley Act of 2002, commonly called SOX or Sarbox, requires all publicly-held U.S. companies to evaluate and disclose the effectiveness of their internal controls as they relate to financial reporting and implement internal controls that ensure security, integrity and reliability of the systems that manage and report financial data.

Under these and other U.S. data security and privacy laws and regulations, the U.S. customer, just as with U.S. export controls, bears the responsibility for compliance on behalf of itself and the offshore performing entity and may not transfer this liability to the offshore performing entity. In other words, the U.S. customer cannot delegate regulatory compliance to the Indian service provider. Both the healthcare and financial services industries in the U.S. have adopted an offshore strategy to achieve business efficiencies and therefore invariably implicate concerns over data privacy and compliance with U.S. laws.

**EU Approach to Data Privacy**

In the European Union ("EU"), data privacy laws are even more stringent than in the U.S. Unlike the U.S., which uses an industry-specific approach for data privacy, the EU has adopted a comprehensive omnibus directive on data privacy that sets the general standards for, among other things, the transfer of personal data from an EU to a non-EU country and prohibits data transfer to a non-EU country whose data protection laws are not deemed "adequate," unless the non-EU country establishes "safe harbor principles" to ensure protections that are needed by EU companies. Because the U.S. is deemed by the EU to be lacking "adequate" privacy protection, the U.S. has established the U.S.-EU safe harbor program which facilitates trans-Atlantic data flows and purports to assure compliance with EU standards by organizations processing EU data in the U.S. U.S. companies voluntarily enter the program by certifying to the U.S. Department of Commerce that they will uphold the safe harbor principles. Since the safe harbor principles are more stringent that the prevailing U.S. privacy standards, the cost of implementation and compliance is not insignificant.

India's current data privacy regime does not meet the EU's adequacy standards nor has India established a safe harbor program to comply with
the EU dictates. Consequently, EU companies are severely restricted from offshoring services to India that involve EU personal data and absent reform India risks marginalization in the European market.

**Recent Incidents of Data Misuse in India**

Recent incidents in India involving breaches of data security have received considerable public attention worldwide and have brought this issue to the forefront in India. In 2003, an employee at an Indian medical transcription company providing services to a U.S. healthcare company threatened to post confidential medical records of patients on a publicly accessible website unless he received a cash payoff from the company. In 2005, three employees of Mphasis, an India-based call center for Citibank, were arrested for allegedly stealing over $350,000 from four Citibank customers in the U.S. by acquiring passwords to customer accounts and transferring customer money to their own accounts. In another event the same year, an employee of Infinity e-Search, a Delhi-based company, was caught allegedly peddling the personal data of over 1000 customers of a UK bank for approximately $8000, casting doubts on the integrity of India's call centers. While such data misuse can and does occur in other parts of the world, these incidents (albeit isolated) created bad publicity and put India in the spotlight by highlighting the lack of an effective legal framework in India to prosecute and effectively deter data misuse.

**India's Existing Legal Framework for Data Privacy**

To date, there are no laws that specifically address data privacy in India. Judicial interpretation suggests that the Constitution of India provides an implied "right to privacy" but this right may be invoked only in disputes between a citizen and the state involving the exercise of governmental power resulting in an "invasion of privacy", such as telephone tapping, police surveillance, and like actions. But there is no case law in India that supports the notion of a private entity enforcing a right to privacy against another private entity.

Limited protection against certain types of data misuse is available under India’s Information Technology Act of 2000 ("ITA"). The ITA protects against "computer offences" involving unauthorized access to data on computers and networks, unauthorized downloading or copying of data, or introduction of viruses or other damage to computer systems, examples of which would be hacking and damage to computer source code. The ITA provides for both civil and criminal remedies, ranging from imprisonment for up to 7 years to fines of up to Rupees 1 crore.
(approximately US $220,000 under average 2006 exchange rates) as well as for the creation of a special appellate court to expedite the disposition of claimed violations of the ITA. In addition, relief may be sought under India’s Specific Relief Act of 1963 to enforce specific performance provisions in the contract against the Indian service provider. For example, in the event the Indian service provider is required to destroy all traces of customer data post-processing and neglects to do so, the U.S. customer may sue for specific performance to ensure compliance under the contract.

Limited criminal recourse against data security violations might be available under other Indian statutes, such as the Indian Penal Code of 1860 and the Indian Criminal Procedure Code of 1973, to prosecute incidents of theft and criminal breach of trust and fraud, for example. These laws, however, only extend to offenses against “corporeal” property. Because data almost certainly would not be deemed to be “corporeal” in nature in a dispute concerning data misuse or theft, data cannot be assumed to be “property” under these laws. However, where the data is housed in a physical object or medium, the theft of the medium might be prosecutable. Similarly, although the theft of the data might not be a prosecutable act, the use of the stolen data to commit a subsequent fraud, such as a call center employee using a U.S. customer’s credit card number to purchase goods, would likely be prosecutable under these laws. In addition, as noted above, a common law remedy for breach of confidence in the form of civil damages and injunctive relief might be available if parties have contractual privity or there exists a fiduciary relationship.

Pending Legislative Action to Cure Deficiencies

India is under enormous pressure from private entities and policymakers in the U.S. and the EU to reform India’s data privacy regime. To protect India’s dominant position in the offshoring space, India’s top trade association that represents India’s IT and outsourcing industry (the National Association of Software and Service Companies ("NASSCOM")) has been aggressively lobbying the Indian government to strengthen its data privacy regime. The Indian government has considered various options to ascertain how best to structure India’s privacy laws, including whether to adopt the EU or the U.S. approach. In response to international pressure, in 2003 the Indian government with the help of key stakeholders drafted an omnibus EU-style data privacy bill, but the bill was abandoned over concerns of over-regulation and the cost of implementation by Indian-based businesses. Most recently, India appears to be
considering a U.S.-style hybrid approach to privacy regulation, relying on a mix of legislation and industry self regulation.

In early 2006, the Indian government approved an amendment to the Information Technology Act of 2000 to expressly deal with data privacy issues. This new bill, if enacted by parliament in its present form, would stipulate security practices to be followed by organizations that handle personal data and impose civil and criminal penalties for intentional misuse or negligent handling of personal data. More specifically, the bill would impose liability on organizations for (i) negligence in implementing and maintaining "reasonable security practices" to safeguard sensitive personal data that resides in a computer resource owned or operated by the organization and (ii) disclosing personal data acquired from a data subject to any other person without the data subject's consent and with an intent to cause injury to the data subject. With respect to item (i) above, the bill limits the damages payable to an injured data subject at Rupees 1 crore (approximately US$220,000 under average 2006 exchange rates) and for item (ii) damages are limited to Rupees 25 lakhs (or approximately US$55,000 under average 2006 exchange rates).

Under this new bill, the parties would be able to contractually agree on applicable "reasonable security practices," but if no such agreement was reached the reasonableness of security practices will be determined by the adjudicating authority based on the nature of the information to be protected from unauthorized access, use or disclosure. The bill would also impose liability under the ITA by providing that an "intermediary" (which means an organization that handles or processes personal data) will be liable for any third party information or data made available by it if it conspires or abets in the commission of the unlawful act or if it has actual knowledge that any information or data residing on a computer resource controlled by it is being used to commit the unlawful act but it fails to expeditiously remove or disable access to such data on the computer resource. In other words, under the bill an Indian service provider would not be liable for any data theft or misuse of data under its control unless the U.S. customer whose data is compromised is able to establish that the Indian service provider conspired or abetted in such activity. The bill also would impose civil and criminal liability on any individual who dishonestly, fraudulently or without appropriate authorization, accesses, downloads or copies any data or information from a computer resource.

It remains to be seen if the Indian government and the Parliament will act expeditiously to pass the bill and enact it into law. However, recent highly publicized events and the threat of the Indian outsourcing industry

32
losing millions of dollars in revenue may provide the impetus for expeditious legislative action.

**India's Private Sector Initiatives**

In addition to legislative efforts, the Indian IT and outsourcing industry is increasingly implementing private sector initiatives to address the data security concerns of U.S. companies and to demonstrate India’s commitment to global security practices. As part of these initiatives, Indian companies are implementing international standards, such as BS7799 and ISO17799, to strengthen data security across the board, including network security (security of storage and transmission infrastructure), information security (security of customer information), physical security (security of work areas), personnel security (security against threat from employees), and business continuity and disaster recovery (contingency plans to retrieve information and prevent loss in the case of emergencies). Many companies in India are undergoing SAS 70 audits and implementing improved internal controls to build credibility and create a positive perception of data security in India. Earlier this year, NASSCOM launched an employee registry program to compile a verified national database of IT and BPO professionals in the outsourcing industry geared towards improving recruitment practices and helping employers to weed out rogue employees. This registry is administered by a third party that conducts background checks prior to listing employees in the database. NASSCOM also plans to set up an independent self-regulatory body to establish and enforce best practices for data privacy and security, provide a training component to help outsourcing companies become compliant, and monitor member companies’ compliance with the standards.

**Recommended Practices to Safeguard Personal Data**

In the absence of specific data privacy laws in India, a U.S. customer must use robust contractual mechanisms and internal security measures to protect sensitive personal data going offshore to India. The contractual protections should be carefully defined to make sure that the Indian service provider is sensitive to the U.S. customer’s industry specific requirements and clearly address the responsibility of the Indian service provider not to undermine, and to facilitate, the U.S. customer’s compliance with the federal, state and local laws in the U.S. to which the U.S. customer continues to be subject. In addition, the U.S. customer should also require the Indian service provider to ensure data privacy through security measures that are commensurate with the risk and consistent with internal pol-
icies, customer expectations and applicable laws, and include contractual protections that provide the U.S. customer the right to conduct comprehensive security reviews and audits to measure the Indian service provider's compliance.

Furthermore, the Indian service provider's failure to comply with applicable laws should not only permit the U.S. customer to immediately terminate the contract but also result in unlimited financial consequences to the Indian service provider. Given that this is a developing area of law, the operative KPO contract should contemplate the possibility of changes in the law and address how costs for future compliance with new laws would be allocated. Needless to say, because prevention is better than cure, the customer should conduct thorough due diligence regarding the service provider's track record of maintaining data security. The customer should also perform a risk assessment prior to sending any sensitive data offshore and implement preventive measures similar to those discussed above regarding its trade secrets. In addition, because most security breaches are generated internally by employees, the U.S. 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.

ENFORCEMENT OF U.S. CUSTOMER RIGHTS AND REMEDIES
The enforcement of the U.S. customer's rights and remedies is always a vital concern, and those concerns can be exacerbated when dealing with an offshore provider, particularly one that has few or no meaningful assets in the U.S. against which any judgment could be executed. If the Indian service provider has meaningful assets located in the U.S. and a U.S. plaintiff successfully obtains a judgment in a court of competent jurisdiction, the judgment can be enforced against those U.S. assets. However, even if a dispute with an Indian service provider is adjudicated in the U.S., if the Indian service provider's primary assets are located in India and not in the U.S., the U.S. 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.

Enforcing U.S. Judgment in India
Under the Indian Civil Procedure Code, a U.S. judgment is not directly enforceable in India. Rather, it can only be enforced by filing a fresh lawsuit in an Indian court based on the U.S. judgment, which will be treated as evidence, among other evidence, against the Indian defendant. This process is much more simplified and streamlined with respect to certain
countries designated as "reciprocating territories" by the Indian government. Foreign judgments passed by courts of these "reciprocating territories" can be directly enforced in India by filing execution proceedings and are deemed to be decrees of the Indian courts for enforcement purposes, thereby considerably speeding up the process. The "reciprocating territories" include the UK, Singapore, Hong Kong, Malaysia, Canada, New Zealand, to name a few, but not the U.S.

In India, a lawsuit to enforce a U.S. judgment must be filed within 3 years from the date of the judgment. The lawsuit will likely be aggressively litigated by the Indian defendant and, because the U.S. is not a reciprocating territory, the lawsuit could require years before any relief is actually awarded by the Indian court. Furthermore, the U.S. judgment will not be enforceable in India if it is determined by the Indian court that (i) the judgment was not issued by a court of competent jurisdiction, (ii) the judgment was not issued on the merits of the case, (iii) the judgment appears to be founded on an incorrect view of international law or a failure to recognize Indian law when such law is applicable, (iv) principles of natural justice were ignored by the U.S. court, (v) the judgment was obtained by fraud, or (vi) the judgment sustained a claim founded on a violation of any law in force in India. Only once a judgment is obtained from the Indian court in this proceeding may the U.S. customer seek to attach the Indian service provider's assets in India. This also applies to any injunctive relief (temporary or permanent) issued by a U.S. court that will need to be enforced against a defendant in India.

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

To assess its likely ability to enforce rights and remedies with respect to an Indian service provider, the U.S. customer should perform due dili-
gence 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 U.S. presence and, correspondingly, local assets which would be available for the satisfaction of judgments. Furthermore, to mitigate any enforcement risks, the U.S. 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.

**U.S. Law as the Governing Law of the Contract**

Indian courts recognize private international law principles and will generally enforce choice of law clauses agreed upon by the parties, except under very limited circumstances, such as, for example, if the chosen governing law would violate public policy in India in some way. Thus, in the operative KPO contract between an Indian entity and a foreign entity, the parties may choose foreign law as the governing law of the contract. A U.S. customer must always unambiguously require U.S. law or a particular state's law as the governing law of the contract. A U.S. customer should be aware, however, that Indian courts may nonetheless apply Indian law to adjudicate disputes in certain fields, including disputes involving IP, real property, labor issues, and insolvency, for example, regardless of the governing law stipulated in the contract, thereby limiting the practical realization of the contract's intended protections should the Indian service provider seek protection in an Indian court.

Although an Indian court likely would apply a foreign choice of law provision between a non-Indian entity and an Indian entity, ironically an Indian court cannot also be assumed to apply a choice of law provision in a contract between two Indian entities if the choice of law is non-Indian law. This is a particularly relevant consideration for a U.S. customer considering establishing a wholly-owned subsidiary in India in a Captive KPO that might then enter into contracts with Indian entities for services. Therefore, a U.S. customer must be cognizant of the effect Indian laws might have on the contract terms agreed upon by those parties.

**Forum Selection Tied to U.S. Courts**

Indian courts also generally recognize forum selection clauses, including clauses that require the parties to litigate disputes exclusively in a foreign jurisdiction. To try to avoid becoming embroiled in litigation in Indian courts, a U.S. customer should require that the parties adjudicate
any dispute arising from the KPO transaction exclusively in a U.S. jurisdiction or a "neutral" non-Indian jurisdiction. To be enforceable in India, exclusive foreign venue provisions should be carefully crafted in accordance with Indian law requirements and include express waivers. One exception to an exclusive venue provision that may be beneficial to a U.S. customer would be to retain the right of the U.S. customer to seek injunctive relief in a local court in India under appropriate circumstances, such as to stop an Indian party from the unauthorized use or disclosure of the U.S. customer's IP in India.

It is important to note that the enforcement of venue selection clauses is not without limitation in an Indian court. Even if a contract contains exclusive venue provision, if the Indian service provider seeks protection in an Indian court an Indian court may elect, in its discretion, not to enforce the venue provision but instead to adjudicate the lawsuit in India if it determines that justice will be better served. For example, a U.S. customer could find itself involuntarily in an Indian court if the Indian service provider, notwithstanding the agreement to submit to foreign jurisdiction, initiates an action in an Indian court or seeks an "anti-suit" injunction against the proceedings initiated by the U.S. customer in a foreign court. In such a situation, the Indian court may decide to assume jurisdiction or stay the action, depending on the circumstances of the case. A 2003 decision of the Supreme Court of India\(^\text{45}\) should bring some peace of mind, however. It upheld the parties' selection of a foreign "neutral" court, that is, a court in a country to which none of the parties or the transaction was connected, and denied the "anti-suit" injunction sought by the Indian party in the Indian courts against proceedings in a foreign court on the basis of *forum non conveniens*.

**DISPUTE RESOLUTION STRATEGIES**

To best mitigate the risk of an Indian service provider seeking refuge in an Indian court and being mired in prolonged litigation\(^\text{46}\) and subject to unfamiliar procedures, private arbitration is the preferred means of dispute resolution in a KPO transaction involving India. The benefits of confidentiality of arbitral proceedings and 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.


\(^{46}\) Indian courts are reported to have a backlog of an astonishing 26 million cases. A Survey of India and China in *The Economist*, March 5, 2005.
in India. Therefore, arbitration is emerging as a globally preferred mode of international dispute resolution in commercial transactions.

India is a signatory to the 1958 United Nations Convention on the Recognition and Enforcement of Foreign Awards, commonly referred to as the “New York Convention,” which makes a foreign arbitral award rendered in a “convention” country far easier to enforce in India than comparable court judgments. India has also adopted the Arbitration and Conciliation Act of 1996 (the “1996 Arbitration Act”), which replaced the Arbitration Act of 1940 (the “1940 Arbitration Act”). The 1996 Arbitration Act is based on the model arbitration rules adopted by the United Nations Commission on International Trade Law, commonly referred to as the UNCITRAL model. The 1996 Arbitration Act, among other protections, (i) recognizes party autonomy and grants parties the flexibility to select applicable procedural rules as well as a foreign venue for arbitration, (ii) empowers local judges to stay legal proceedings if the parties have agreed to resolve their disputes through arbitration, (iii) minimizes intervention of the courts in the arbitral process, and (iv) enables enforcement of a foreign arbitral award in India by obtaining an execution decree from a court in India.

The 1996 Arbitration Act delineates certain grounds consistent with the New York Convention under which a foreign arbitral award may be challenged or refused enforcement in India. The grounds include (i) the incapacity of any of the parties to the contract, (ii) the invalidity of the arbitration agreement under the law governing the dispute, (iii) a lack of due process afforded to either party, (iv) if the award is beyond the arbitration clause’s scope, (v) the subject-matter is not subject to resolution by arbitration under India’s laws, or (vi) if enforcement would be contrary to public policy in India. The Indian judiciary has differed on the interpretation of “public policy” in the context of foreign arbitral awards. The Supreme Court of India had held with respect to the 1940 Arbitration Act that “public policy” refers only to the “fundamental policy of Indian law, the interests of India and justice or morality.” The Supreme Court recently reiterated its holding when interpreting the 1996 Arbitration Act.

If an Indian court is satisfied that the foreign arbitral award is enforceable pursuant to the 1996 Arbitration Act, it is deemed to be a decree of that court. An Indian court’s order refusing to enforce a foreign arbitral

---


208
award is appealable as of right but an order upholding the foreign award is not appealable. The 1996 Arbitration Act permits a party to seek interim injunctive relief or other protective orders from an Indian court (for example, seeking the preservation of evidence or to block the sale of contested IP pending the arbitration) before or during the arbitral proceedings, or even after the award is pronounced but before it is enforced, unless the arbitration agreement expressly excludes the right to seek interim relief.

In a KPO transaction, therefore, the contract should unequivocally specify that all disputes relating to the transaction must be arbitrated. The contract should identify the procedures applicable to the arbitration, which can be a selection of AAA International Arbitration rules, International Commercial Arbitration rules, or JAM’s International Mediation and International Arbitration rules, for example. The contract should also specify that all disputes be presented and adjudicated orally and in writing in the English language. The U.S. customer should consider whether it wishes to preserve the right to seek injunctive relief either under the 1996 Arbitration Act or other circumstances specific to the transaction. If not, the contract should specify that as well. The contract should also set forth a neutral venue (such as Singapore, Paris or London) for arbitration outside of India, and preferably in the U.S.

CONCLUSION

In summary, KPO to India can not only yield enormous cost savings and increased efficiencies but also leverage India’s vast knowledge class to perform “high end” skill and judgment based services and functions. The potential KPO customer must be aware, however, that KPO presents a number of risks that must be considered and addressed. These risks can be managed, however, with thorough due diligence and the careful assessment and treatment of the issues discussed above in the operative KPO contract that memorializes all underlying business terms and provides real and practical protections and enforcement mechanisms.

This Mayer, Brown, Rowe & Maw LLP publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek specific legal advice before taking any action with respect to the matters discussed herein.