Business Law Journal | UC DAVIS SCHOOL OF LAW

Archives About Join Contact Submissions Subscriptions Symposium

Barbara Crutchfield George

.

Deborah Roach Gaut

.

Offshore Outsourcing to India by U.S. and E.U. Companies
Legal and Cross-Cultural Issues that Affect Data Privacy Regulation in Business Process Outsourcing

Barbara Crutchfield George
Deborah Roach Gaut

Posted Monday, May 1, 2006
6 U.C. Davis Bus. L.J. 13 (2006)

I. INTRODUCTION

A natural economic consequence of our rising globalized society is that American companies have outsourced business process functions to offshore locations. This raises a multitude of cultural, political, social, and legal issues. India is one of these important offshore locations. According to some estimates, India controls 44% of the global outsourcing market of software and back-office services.[1] India has become the host outsourcing country of choice for many U.S. companies. This is due to the economic advantages and the large supply of a well-educated, highly motivated, competent, productive, and English-speaking workforce. Much attention has been centered on the issue of the economic effect on Americans who have lost their jobs because companies have outsourced work to foreign locations.[2] However, with offshore business process outsourcing ("BPO") firmly entrenched,[3] data privacy protection has risen to the forefront as a critical concern for Americans because of the risks of misuse inherent in the export of extensive amounts of sensitive personal information[4] about the customers of the outsourcing U. S. companies.[5] In India, these risks are particularly heightened because the country lacks legislative and regulatory protection of data privacy.

Due to outsourcing practices today, employees of Indian service providers have access to extensive personal information about customers of American companies. This includes credit card numbers, social security numbers, driver's license numbers, dates of birth, and other important personal information that has the potential for misuse. Indian employees of BPO service providers engage in several tasks that expose them to sensitive private data in transactions. Indian employees handle tasks such as the transcription of medical records, preparation of tax returns, processing of credit card applications and bills, handling of mortgage applications, reviewing of insurance claims, analysis of patients' X-rays, and help-desk services. U.S. companies would be remiss to ignore that "[t]hese kinds of [business process] applications create thorny issues about personal data protection for [U.S.-based] customers....As offshore vendors deal more often with customers and specific customer data, the potential for abuse rises."[6]

Currently, no data privacy protection legislation of any kind exists in India. Therefore, American outsourcers rely upon contractual obligations and the internal security measures taken by Indian service providers for protecting nonpublic information. Although the Indian Ministry of Information Technology and the National Association of Software and Service Companies (NASSCOM) proposed amendments in 2004 that cover data privacy,[7] the Information Technology Act, enacted in 2000 ("IT Act of 2000"), does not specifically provide for protection of sensitive personal information.

A specter is immediately raised regarding East-West cross-cultural differences in emphasizing the importance of protecting private data for companies in India that are engaged in BPO functions.[8] These differences can have a substantial impact on the enactment and enforcement of adequate privacy laws, the level of importance, and the seriousness that data privacy protection is given. In addition to India's perspectives on data privacy, other complicating factors affecting the draft of an adequate data privacy law include the cultural and legal clashes in the way data privacy is treated in its major outsourcing targets - the U.S. and Europe.

The comprehensive European Union Directive on Data Privacy ("E.U. Directive") plays an important role for U.S. multinational companies. The E.U. Directive is relevant to the final resolution of the legislative, or "Safe Harbor," approach that India ultimately may adopt.[9] In order to do business with E.U. Member States, the E.U. Directive requires that India provide an "adequate" level of data privacy protection.[10] Any legislation passed by India will have to meet the E.U. standard or, in the alternative, India will have to enter into a "Safe Harbor" agreement with the E.U. It is noteworthy that the U.S. has adopted a sector approach, rather than a comprehensive approach, in its own data privacy protection measures.[11] The U.S. approach does not itself meet the "adequacy" test of the E.U. Directive so it has used the "Safe Harbor" approach to solve its own problems with the European Union.[12]

India's cultural history is a significant factor for American outsourcers to consider in pressing for either data privacy legislation in India or protective contractual provisions with Indian companies. Indian cultural history may affect Indian companies' interpretation of the concept of privacy, which will affect the degree of importance that India as the host country is willing to place on the protection of privacy. A pertinent statement appears in The European Union's Assessment of Adequacy, a report addressing the effect of differing political and cultural values on interpretations of standards of "adequacy" of data privacy protection measures to meet the E.U. standards:

A final difficulty is that of cultural and institutional non-equivalence. Judgments about adequate protection must remain sensitive to important cultural differences. Despite the growing convergence of international data protection policy, 'privacy' still means something very different in various cultural and national traditions, perhaps particularly in non-Western jurisdictions but by no means there alone....[13]

Within the broad context of the effect of cultural differences inherent in doing business in India, this article begins with Section II, which discusses the background that led to the current surge of outsourcing to India. Section III is a demonstration of the data privacy risks in India through a narration of several recent incidents involving misuse of personal data by employees of Indian service providers. Section IV examines the manner in which sector data privacy laws in the U.S. and the omnibus E.U. Directive affect ongoing relationships with Indian service providers. Section V reviews the attempts towards legislative action on data privacy protection in India in the last decade. Section VI analyzes the research examining cross-cultural differences that must be bridged in order to integrate existing regulatory models into the Indian approach to data privacy. Section VI also presents a pragmatic legal and political interpretation of the research on data privacy and regulatory models. Section VII offers recommendations for addressing protection of data privacy in India from (1) an international perspective, (2) a national perspective for the U.S. and India (as the domicile of the outsourcers and service providers respectively), and (3) from a company-level perspective. Finally, in Section VIII, the authors conclude that, although a powerful market incentive for Indian companies is recognition that any major leak of sensitive information could destroy their competitive position, this same recognition should be a basis for driving enlightened debate in India regarding appropriate regulatory or legislative action.

II. BACKGROUND LEADING UP TO THE CURRENT SURGE OF OUTSOURCING IN INDIA

Offshore outsourcing of U.S. business processes and information technology to India began in the late 1980s. General

Electric ("GE") was one of the first American companies to take advantage of outsourcing opportunities in India. In September 1989, Jack Welch, Chairman and CEO at the time, met with the Chief Technical Advisor to then Prime Minister Rajiv Gandhi, who convinced Mr. Welch of the opportunities for GE in India.[14] Within a year, GE formed a joint venture with Wipro Ltd., to develop and market medical equipment in India.[15] In recognition of India's potential, Mr. Welch was quoted as saying, "India is a developing country with a developed intellectual capability."[16] GE then began to use India as a base for data entry, credit card application processing, call centers, and other consumer interaction activities.[17]

India's foreign business opportunities were limited until the Indian government began to open up its economy and to dismantle tariff and export controls in 1991. Dr. Manmohan Singh, then India's Finance Minister (now India's Prime Minister), began opening the Indian economy for foreign investment and introducing competition into the Indian telecom industry to bring down prices.[18] To attract more foreign investment, Dr. Singh, an economist, made it much easier for companies to set up satellite downlink stations.[19] Prior to that time, if a foreign company had its own satellite downlink, an Indian government official was required to oversee it and had the right to examine all data going in or out of the country.[20] With the newly relaxed rules instituted by Dr. Singh, satellite downlink stations were established in Bangalore.[21] Foreign companies could then avoid the unpredictable Indian phone system and connect with their home bases in America and other distant locations.[22]

In one of his early trips to India, GE's Jack Welch envisioned India's future in his statement that, "I saw India as a huge market, with a rapidly growing middle class of 100-plus million people out of an 800 million population. The Indian people were highly educated, they spoke English, and the country had lots of entrepreneurs trying to break the shackles of heavy government bureaucracy."[23] Since then, Citigroup, Microsoft, Delta Airlines, IBM, Accenture, and countless other American multinational companies have developed outsourcing relationships with leading Indian outsourcing companies, such as Infosys Technologies, Wipro , MphasiS, and Tata Consulting.

The vast untapped talent in India was more formally discovered with the advent of Y2K. India provided the large number of qualified technicians who would engage in the tedious task of reviewing and readjusting many U.S. computers.[24] After the occurrence of Y2K, U.S. e-commerce businesses were at their apex, while there were an insufficient number of qualified engineers in the U.S. Thus, with the recent positive business outcomes the U.S. had experienced with Y2K work done in India - and with so many English-proficient[25] engineers available - American companies again turned to India to augment its workforce.[26] Many Indian engineers came to the U.S. on temporary work visas, but they had to return home when the dot-com bubble burst.[27] American companies felt the economic pinch at the end of the dot-com era and in looked for ways to reduce their costs. U.S. managers once again turned to India where they had worked with companies so successfully during the panic of Y2K. People in India who had worked on the Y2K project and Indians who worked on temporary visas in Silicon Valley (and had since returned to India) had experience and knowledge in the American way of doing business. This combination of factors allowed companies to create an entirely new form of outsourcing collaboration to tap the pool of talent in India through the PC, Internet, and, most importantly, the newly laid, underwater fiber-optic cable. As Thomas Friedman, author of The World is Flat, asserted in his widely read book on globalization, the undersea fiber-optic cable allowed "any service, call center, business support operation, or knowledge work that could be digitized [to] be sourced globally to the cheapest, smartest, or most efficient provider."[28]

Even though India is currently classified as a "developing nation," its people are anxious to take advantage of their new connection to the world as they begin to fully recognize the potential global value of their business resources. Three assets make India a natural choice for offshore outsourcing: English language fluency among most managers and mid-level employees; the aggressiveness of Indian companies; and a low-cost workforce. Additionally, India has all of the necessary components for a compatible match with American companies for information technology and business processing outsourcing. India also has a democratic form of government. As a British colony for two hundred years, the country reflects the familiar lines of the British common law system and has a large number of educated middle-class citizens[29] who speak fluent English. Since the cost of living is one-fifth of the cost in the U.S., the cost of labor is far less in India than in the U.S. India also has one of the most developed educational systems in the world, with seven prestigious Indian Institutes of Technology (IIT) and four equally prestigious Indian Institutes of Management (IIM).[30] India has the youngest population in the world with almost 70% of its population below the age of 35 and 50 percent under the age of 25, which provides an almost unlimited number of potential workers.[31] At the time of this writing, 800,000 Indian workers are estimated to be employed in all areas of the outsourcing service industries. [32] Furthermore, a reputed 400 Indian businesses engaged specifically in providing BPO services, with a workforce of 400,000 workers.[33] Outsourcing is most prevalent in the cities of Mumbai and Hyderabad, but Bangalore,[34] known as the "Silicon Valley of India," has garnered a large portion of the business.

In November 2004, India's outsourcing boom appeared to face a crisis when Senator John Kerry referred to "Benedict Arnold companies and C.E.O.'s" that sent jobs overseas during the months leading up to the U.S. presidential election. [35] Mr. Kerry had promised that, as President, he would end tax deferrals for companies that sent work abroad.[36] His election would have produced a sharp decline in outsourced jobs from the U.S., so India's outsourcing companies were jubilant with the results of the November 2004 elections that kept President Bush in office.[37] The confidence that Indian businesses exhibited toward Mr. Bush was reinforced in the January 2005 "Economic Report of the President," which specifically referred to India as an example of an outsourcing destination.[38] The report also stated that "when a good or service is produced more cheaply abroad, it makes more sense to import it than to make or provide it domestically."[39] President Bush's report certainly declared his commitment to a continuation of his administration's encouragement of offshore outsourcing by American companies, and contained a strong endorsement of India as an outsourcing destination.

III. DATA PRIVACY RISKS

In the U.S., the main objection to offshore outsourcing has been that jobs are being sent overseas.[40] However, the sensitive personal information that leaves the country presents a grave risk for Americans.[41] U.S. companies have a duty to shield their customers from the possibility that their private personal data will be misused by employees of a foreign service provider. People who live in the U.S. have become more cognizant (and fearful) about breaches in data privacy that have resulted in identity theft because of broad newspaper and television coverage of several incidents, including hackers tapping into 40 million credit cards at Atlanta-based CardSystems, Inc.[42]; major security lapses at ChoicePoint Inc.[43] and Bank of America[44]; and the loss of financial information for 3.9 million Citigroup customers by United Parcel Service.[45] With this heightened sensitivity to the dangers of identity theft occurring within the U.S., it is understandable that American businesses and consumers have become nervous about personal information that now is accessible to thousands of workers in India through business process outsourcing.

To date, no data privacy protection laws (comprehensive or sectoral) currently exist in India, and no counterpart to the Federal Trade Commission has been established to issue, administer, and enforce data privacy rules. Data privacy risks abound for U.S. accounting firms that outsource tax returns for preparation in India, and for hospitals that electronically send medical records overseas for quick transcription.[46] Additional examples of BPO functions in which access to an American client's private personal information exist include processing credit card and mortgage applications, reviewing insurance claims, processing bills, analyzing and transcribing medical records (e.g., X-rays sent via the Internet for analysis in India), and assisting customers via help desk services. If credit card information is stolen and used, a 12- to 15-hour time zone difference between the U.S. and India can allow a culprit in India to use the card while the card owner is still sleeping.

The risks are increased for Americans because U.S. federal laws do not apply to foreign companies operating overseas. There is no guarantee that data privacy legislation will be enforced even if it is passed in India. Therefore, private parties must continue to ensure protection of their consumers through contractual provisions and security measures. If a U.S. plaintiff can successfully obtain a judgment in a court with jurisdiction and the Indian service provider has assets in the U.S., the judgment can be enforced against those U.S. assets.[47] Even if India did have data protection laws, it would be difficult for Americans to use Indian courts to sue their domestic companies for problems arising from the misuse of American data.[48] Indian courts cannot be used to pursue claims based on U.S. laws. Additionally, U.S. citizens cannot use U.S. courts to pursue claims of misuse of personal data by an employee of a company domiciled in India. Even if India adopts data privacy legislation, redress for Americans would lie with the Indian legal system. Timely enforcement could prove difficult, given the reputedly slow pace of the country's legal system.[49]

A. INCIDENTS OF MISUSE OF DATA BY INDIAN BUSINESS SERVICE PROVIDERS

Overall, few incidents of misuse of data by employees of Indian business service providers have arisen to date. However, the few that have occurred have set off alarms for both American and Indian companies. For example, in June 2005, American business outsourcers and their Indian counterparts were extremely concerned when Interpol was asked to investigate allegations that a 24-year-old worker at Infinity eSearch, a web marketing company in New Delhi, had sold information that he obtained from call center workers at a BPO company.[50] An undercover British reporter from a London tabloid newspaper, *The Sun*, claimed that the Infinity e-Search employee sold him Barclay Bank account details for 1,000 U.K. customers.[51] The account holders' secret passwords, addresses, phone numbers, and passport details were allegedly sold for 350,000 rupees (INR 350,000), which is the equivalent of around U.S. $8,000. As a basis for comparison, the annual per capita income of India's 1.05 billion inhabitants is about INR 20,210 or U.S. $470.[52] Additionally, it has been estimated that an entry-level call center employee in India receives an average annual salary of U.S. $12,000[53], which exceeds the salaries of many early-career Indian teachers, accountants or lawyers.[54] This situation points out the flaws in having sensitive information in the hands of offshore employees in a developing country where the temptation may be great to make vast amounts of money in local currency by selling information to unscrupulous buyers, particularly when the exchange rate makes the purchase cost in the western country relatively minimal. [55]

A spokesperson for the Amicus union in the U.K. said that the union had issued general warnings about the data protection implications of outsourcing financial services
abroad, and that "[c]ompanies that have offshore jobs need to reflect on their decision and the assumption that cost savings benefiting them and their shareholders outweigh consumer confidentiality and confidence."[56] On the other hand, Saurav Adhikari, Corporate Vice-President (Strategy) at HCL Technologies in India, has argued that "[g]iven the strong credentials of the Indian industry, this incident would be a blip on the BPO radar at best, and will result in the industry raising the bar."[57]

Another serious case of the mishandling of confidential information occurred in April 2005, when Indian police arrested several men who had worked for a MphasiS call center for Citibank and number of their associates.[58] The former employees of MphasiS (in the city of Pune, located near Mumbai) were charged with misusing financial data and illegally withdrawing money from the Citibank accounts of New York customers. The MphasiS employees had obtained bank customers' PIN numbers and other account details, which allowed them to log into Citibank's online system and transfer approximately $350,000 - $425,000 out of the customers' accounts.[59]

Additional illustrations of the misuse of data include:

· In 2003, Indian employees, who were working on medical records for Ohio's Heartland Information Services, threatened to release confidential records unless they received a cash payoff from the company.[60]

· In 2003, an Indian programmer working for India's Geometric Software Solutions Company tried to sell a source code from SolidWorks (its U.S. buyer) to another U.S.-based company.[61]

· In 2004, an Indian employee, who was working at a call center in Noida, India, used an American's credit card to buy extensive electronics equipment from Sony.[62]

· In 2005, a series of events similar to the incident with *The Sun* occurred with the alleged sale of sensitive personal data to undercover Australian Broadcasting Corporation reporters for the equivalent of less than U.S. $8 per person. [63]

While reports of fraud and theft of data in India have been rare, any report of misconduct serves as a reminder that misuse of sensitive personal data by offshore service providers may pose an imminent and serious threat.

B. INDIAN SECURITY EFFORTS

It can easily be ascertained from the actions taken by Indian service providers, as well as comments and recommendations emanating from NASSCOM, that both groups are very conscious of the problems that can emerge if major security abuses arise concerning nonpublic personal information. Strict measures have been adopted by many Indian businesses to prevent their employees from misusing customers' personal information.[64] NASSCOM has been active in trying to encourage the Indian legislature to pass amendments to the 2000 IT law to cover data privacy, along with other efforts to emphasize the importance of data privacy protection.[65]

1. INDIAN SERVICE PROVIDERS

Many BPO service providers in India have engaged in voluntary control (i.e., self-regulation) and have adopted stringent security measures to reduce the risks of misuse of nonpublic personal data.[66] One of the four call centers currently run by ICICI OneSource, which employs 4,000 young Indians to process credit-card bills and make telemarketing calls for U.S. and European companies, looks like a "fortress" to those who witness procedures of entry. [67] At another company, TransWorks Information Services (a Mumbai-based BPO and call centre company), C.E.O. Prakash Gurbaxani stated, "[o]ne of the things you do, for example, is that you make sure that the agent workstation has no other software than is required for the job, has no internet access that could be potentially used to e-mail, say, a credit card number to someone else. You also need to ensure that the office is paperless so that no data can be copied out."[68]

To reduce the risks of misuse of nonpublic personal data, some BPO companies in India also have adopted one or more of the following stringent security measures:[69]

· Armed guards are posted outside offices.
· Entry is restricted by requiring microchip-embedded swipe cards.
· Bags and briefcases are prohibited in the work area.
· Computers in workstations have no printers or devices for removable storage.
· Agents/visitors are banned from carrying mobile phones to the production floor.
· Phone calls to and from either family or friends are forbidden in employee workstations.
· Image capturing devices like cell phones, scanners or photocopiers are not allowed.
· Internet and e-mail access are prohibited at workstations and inside most BPO companies.
· Key information, such as passwords that clients provide, is encrypted and, thus, is unseen by employees.
· Employees are monitored via closed-circuit television.

These protections, which have been taken to tighten security, are an attempt to ease customer concerns over theft of private information.

2. TRADE ASSOCIATION SECURITY EFFORTS

NASSCOM held its first annual conference on cyber-security with its U.S. counterpart, the Information Technology Association of America (ITAA), in October 2004 in New Delhi.[70] NASSCOM's objective was to project India as "a 'trustworthy sourcing center' in the area of data privacy and information security."[71] NASSCOM has helped to establish designated cybercrime sections within police departments and is the primary funding agency for special training of at least a dozen police offices in Mumbai.[72] Also, the trade association has engaged the services of an agency to prepare a national database of India's approximately 350,000 call center workers so employers can quickly ascertain from the records whether hiring a particular applicant will pose a security risk. [73] At the time of this writing, NASSCOM had plans to create and maintain a list of people who may be unfit for future employment (i.e., a blacklist). [74]

C. OTHER INTERNAL PROBLEMS IN INDIA THAT IMPACT SECURITY

India has a number of other problems that affect protection of sensitive personal information. These include weak law

enforcement, perception of business corruption as reflected in India's ranking by Transparency International, infrastructure problems and political risks.
An example of India's weak law enforcement was demonstrated in the 2004 theft of a source code at the Bombay development center for Jolly Corp., a San Carlos, California-based, photo ID card creator, and print software vendor that opened a subsidiary in Mumbai, India.[75] An employee in India uploaded and e-mailed files containing the source code and sent them out to her Yahoo e-mail account.[76] When Mr. Jolly went to the Cyber Crime unit of the Mumbai Police, he claimed that the unit refused to investigate.[77] "The law is very weak in India,…low level police in India don't really know what a computer is, and…[t]he authorities have refused to do anything until they are paid a bribe."[78] In August 2004, Mr. Jolly sued the Mumbai police for their negligence in refusing to investigate the alleged theft of the proprietary source code.[79] This scenario demonstrates the frustration that can be encountered by American businesses that attempt to work within the law enforcement framework of another country.
Business corruption is also perceived as a problem in India. The latest figures from Transparency International (TI),[80] the leading global nongovernmental organization devoted to eradicating corruption, support the premise that extensive business corruption is perceived to exist in India. This situation does not instill confidence for American businesses that outsource to India. The October 2005 TI Business Corruption Perception Index ranked (with 10 being least corrupt) the U.K. as number 11 with a score of 8.6, the U.S. as number 17 with a score of 7.6 and India as number 88 with a score of 2.9.[81]
Additionally, indescribable infrastructure problems must be overcome to make conducting business easier in India. Even though the country is currently undergoing massive infrastructure building that is creating a fundamental transformation in many urban pockets throughout India, extensive uncertainties still exist in the areas of roads, airports, water and sewage systems, telecommunications, and electricity - to name a few.
Finally, political risks should not be overlooked because any major breakdown in the political arena can cause disruptions for BPO providers in India. Instances in which political instability can arise are:
· Relations between India-Pakistan over the testing of nuclear missiles.
· Relations between India-Pakistan over the Kashmir border dispute.
· Problems with separatist groups within the country.
· An increase in the number of terrorist attempts to undermine India's successful partnerships with the West.[82]

In evaluating such country risks for U.S. financial institutions, the Federal Deposit Insurance Corporation has recommended that institutions "closely monitor foreign government policies as well as political, social, economic, and legal conditions in countries where they have a contractual relationship with a service provider."[83]

IV. DATA PRIVACY LAWS THAT DIRECTLY AFFECT CONTINUING RELATIONSHIPS WITH INDIAN SERVICE PROVIDERS

In order for India to protect its competitive position, the country must meet the privacy expectations of outsourcing companies in countries abroad. At present, India faces a serious problem with meeting the adequacy standards of the E.U. Directive. Additionally, U.S. companies are putting pressure on the companies with which they do business to protect their customers against identity theft.[84]
As stated earlier, only a few instances of misuse of data by employees in Indian companies have emerged, but as the industry grows,[85] chances for abuse increase exponentially. To date, the U.S. has not experienced any broad media coverage of data theft in India. However, as previously discussed, the U.K. saw front page coverage of what appeared to be a "sting" operation in which an Indian outsourcing employee sold to an undercover British reporter from *The Sun* the bank account details of 1,000 U.K. customers.[86]
When companies in the U.K. and the U.S. realize that the Indian parliament has not considered data privacy a serious enough matter to pass a proposed amendment to its 2000 Information Technology Act, the companies can easily begin to lose confidence, particularly at a time when consumers have a heightened awareness of the dangers of identity theft. It is a questionable practice for U.S. companies to solely rely on contractual provisions between companies for protection.

A. EUROPEAN UNION DATA PRIVACY DIRECTIVE

Another model which provides a more compelling reason for India to consider passing data protection legislation is the 1995 E.U. Directive.[87] The E.U. Directive is a comprehensive data protection law that orders its member states to establish a legal framework to protect the fundamental right to privacy with respect to processing personal data that has extraterritorial effect.[88] India, which has no data privacy protection legislation at this time, faces problems regarding the E.U. Directive's requirement that personal data can be transferred only to third countries providing "adequate protection" for that data.[89] The European Union has deemed India to be non-compliant with its privacy rules.[90] Until India is in compliance, companies in the E.U. Member States are heavily restricted as to the types of activities that can be performed by Indian service providers.[91]
India must either adopt comprehensive legislation or establish the Safe Harbor Principles to receive personal data from an E.U. Member State.[92] Either a data privacy law or certification to the Safe Harbor Principles with the E.U. will indirectly ensure protections that are needed by American companies. The E.U. will not be satisfied with offshore outsourcing to India until the latter has passed comprehensive data privacy protection legislation. This is because the strict data privacy rules in Europe make it clear that they have a deep-seated preference for legalistic regulatory models as opposed to market mechanisms.[93]

1. EXTRATERRITORIAL EFFECT

The E.U. Directive establishes strict rules about whether and how a controller may transfer personal data from the E.U. to a non-E.U. country.[94] The basic principle in Article 25 requires E.U. Member States to prohibit the transfer of personal data that will undergo processing in a third country if that country fails to provide "an adequate level of protection."[95] Thus, private companies could be prevented from transferring personal information outside the E.U. to India. The E.U. Directive does not define what constitutes an "adequate" level of protection, but it indicates that all circumstances surrounding the transfer, including the laws in force in the third country, must be considered by the supervising authority in making a determination about adequacy. [96]
Presently, the U.S. has its own problems in meeting the E.U.'s requirements of "adequacy" because it does not have comprehensive federal legislation protecting data privacy.[97] After two years of discussions between the U.S. and E.U. the U.S. Department of Commerce issued the Safe Harbor Principles in 2000.[98] The E.U. approved data protection framework allows a U.S. company to become Safe Harbor-accredited by self-certifying and declaring that it will comply with the seven Safe Harbor Principles.[99] The anxiety of the U.S. over the extent of India's data privacy protection will be reduced if India passes legislation that meets the E.U. Directive regarding the "adequacy" standard.

B. U. S. LEGAL AND REGULATORY ENVIRONMENT

At the time of this writing, the U.S. relies on a combination of legislation, regulation, and self-regulation to provide data protection. However, no comprehensive U.S. data protection legislation exists. As a result, the current generation of sector-specific U.S. data privacy laws fails to protect American consumers from many types of privacy breaches. Examples of sector-related legislative enactments and regulatory standards that are used in the U.S. to protect data privacy relevant to offshore BPO are included in Appendix A.

V. STATUS OF LEGAL PROTECTION PROVIDED FOR DATA PRIVACY IN INDIA

Currently, India has no legislative enactments or regulations applicable to data privacy protection. When U.S. customers look for methods of legal recourse in India for abuse of data privacy, they find that the IT Act of 2000, which is the only

legislation covering electronic commerce, does not apply. Pavan Duggal, an Indian cyber law expert and Supreme Court advocate, has argued strenuously that India should adopt stringent cyber laws for preservation of confidentiality and strict punishment for cyber crimes.[100] Duggal emphasized that, until a tighter data protection legal regime is in place in India, foreign customers can only rely on contractual obligations for protecting and preserving data.[101]

A. 1998 IT ACTION PLAN: INDIA'S FIRST ATTEMPT TO INCLUDE DATA PRIVACY PROTECTION

In the late 1990s, an unsuccessful attempt was made to include protection of data privacy in India's pending information technology legislation. The National Task Force on IT and Software Development submitted an "IT Action Plan" ("Plan") to then Prime Minister Vajpayee.[102] Using the U.K. Data Protection Act as a model, the Plan called for the creation of a "National Policy on Information Security, Privacy and Data Protection Act for handling computerized data."[103] This effort only realized partial fruition in the passage of the Indian Information Technology Act of 2000, which covers unauthorized access and data theft from computers and networks, but fails to cover privacy and data protection issues. [104]

B. INFORMATION TECHNOLOGY ACT, 2000

The IT Act of 2000 ("Act") contains language which provides "legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as 'electronic commerce'."[105] The relevant part of the Act imposes liability "to pay damages by way of compensation not exceeding one crore rupees [INRS 10M or approximately $230,000] to the person so affected"[106] if "any person without permission downloads, copies, or extracts any data, computer database or information from such computer, computer system or computer network."[107] Criminal offenses include (1) tampering with computer source documents,[108] (2) hacking into computer systems,[109] and (3) publishing obscene information in electronic form.[110] Chapter X creates a Cyber Appellate Tribunal to oversee adjudication of cybercrimes, such as damage to computer systems and breaches of confidentiality. [111]

C. PROPOSED AMENDMENTS TO THE INFORMATION TECHNOLOGY ACT, 2000

NASSCOM has suggested new data protection clauses for the Indian government to incorporate in IT Act of 2000.[112] One of the provisions under the proposed legislation allows local police to take additional measures to enforce data protection.
Section 66 in the Act would be renamed "Computer-related Offences."[113] Rodney D. Ryder, legal advisor to the Indian government on the IT Act of 2000 stated, "the proposed legislation will not just ensure data protection, but would also pave the way for appointment of a regulator to monitor the collected data and its usage."[114] He also predicted that "[i]t is somewhat similar to a data protection or data privacy commissioner in Europe who would look into how the data is collected and how it is used."[115]
The Indian Parliament was expected to act on the proposed amendments in the Fall of 2004, but seems to be moving slowly. An expert committee was appointed to examine important issues regarding data protection in January 2005. [116] In June 2005, the London's *Sun* newspaper allegation that an employee in an Indian call-center sold the personal information of 10,000 Barclay Bank customers may be the catalyst that spurs the legislature to amend the IT Act of 2000.[117] Media coverage of this incident was considered potentially damaging enough to cause the intervention of Indian Prime Minister Manmohan Singh.[118] After the information was made public, Prime Minister Singh immediately instructed government officials to hasten the amendments to the IT Act of 2000 for which NASSCOM has been pressing for the last two years.[119]
Perhaps the legislature's slow progress in amending the IT Act of 2000 did not arise from strictly legalistic concerns. A special article written for the *Economic and Political Weekly* in Mumbai, India, contained a telling criticism of the IT Act of 2000 in which the writer complained that "in [the legislature's] desperate need to bring in some security for activity on the net, it relies heavily on the executive, little realizing that it can result in violation of civil rights.âÄ¦" [120] The discontent surrounding the IT Act of 2000 is reflected further in the statement that the Act "demonstrates a legislature deeply skeptical of the internet, rooted in the conventions of the past, yet battling with the need for an information technology law in the present-day circumstances."[121]

VI. CROSS-CULTURAL DIFFERENCES IN EXISTING REGULATORY MODELS OF PRIVACY PROTECTION: A SOCIAL-SCIENTIFIC PERSPECTIVE

The *very words* "international regulation" and "data privacy" themselves carry different connotative (i.e., emotional or personal) meanings for people from different countries in order to understand the reasons that cross-cultural differences exist in current regulatory models of privacy protection for the U.S., E.U., and India. These differences primarily arise from the unique language and culture of the people (i.e., nation) with whom one may be negotiating.

A. INDIA'S FLUENCY WITH THE ENGLISH LANGUAGE

The ability of large numbers of middle and upper class Indians to speak English has given them a great advantage in providing business process services for companies in the West. The emphasis on English as a second language began as early as the 1800s, when Raja Ram Mohun Roy promoted acceptance of the English language "as a vehicle of Western thought and knowledge for the future benefit of India."[122] It was somewhat prophetic that he was known as the "Father of Modern India'.[123] One of India's Governor/Generals during Raja Roy's time was Lord William Bentinick, who took another step towards embedding the English language into Indian life and culture by channeling the official education policy towards "imparting to the Native population knowledge of English literature and science through the medium of the English language."[124] An important step taken during that era was the replacement of Persian by English as the official language of the higher law courts (and by regional languages in the lower courts).[125]
Today, Raja Roy's vision is evident since India ranks among the top three English-speaking countries in the world with over 30 million speaking the language.[126] This change can be attributed to its history as an English colony. English is the main language of instruction in many schools, with some or all coursework taken in English. It is the second language of most of the educated population and the "link language" between residents of different states where more than 30 different primary languages are spoken[127]
Although English is widely used as a second language in India, inherent difficulties arise in arriving at a common understanding of a concept such as "data privacy." True communication does not take place without a full understanding of the culture and background of the language spoken. This linguistic fact of life is easily illustrated with the commonality of English as the first language amongst people of the U.S., Australia, Canada, and the U.K., but with each country having its own unique background that determines the ways in which its citizens express and understand the same concept.[128] Thus, it is not hard to imagine that there are probably opposite reactions between an American in Washington, D.C., who shudders upon hearing the word "identity theft," and an Indian living in New Delhi who may shrug upon hearing the same term.

B. CROSS-CULTURAL DIFFERENCES IN INTERNATIONAL REGULATORY MODELS OF DATA PRIVACY PROTECTION: THE "NATIONAL CULTURE" APPROACH

In order to understand the dynamic relationships among history, language, and culture, one may benefit from an examination of Hofstede's seminal work on cross-cultural differences in national cultures. Coupled with two studies by Sandra Milberg and her associates, a complex picture emerges of the relationships between dimensions of national culture and international regulatory models of data privacy.

1. HOFSTEDE'S THEORY OF CULTURE

According to Geert Hofstede, culture is "the interactive aggregate of common characteristics that influences a human group's response to its environment. Culture determines the identity of a human group in the same way as personality determines the identity of an individual."[129] It emerges over time as a function of a society's geographic location, physical climate, history, economy, political systems, religious influences, education systems, technologies, and shared language âÄ" among other important variables.[130] In contrast to nation states, whose borders are tangible and transitory, cultures are intangible and far more enduring.
In his book, entitled Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations across Nations, Hofstede identified five distinct dimensions of human behavior that characterize a culture: (1) power distance, (2) uncertainty avoidance, (3) individualism/collectivism, (4) masculinity/femininity, and (5) long-term or short-term orientation. *Power distance* is defined as how a culture approaches and accepts inequality in status (i.e., prestige, wealth and power).[131]*Uncertainty avoidance* is characterized as the ways in which a culture handles uncertainty in the future, particularly "through the domains of technology, law, and religion. In organizations these [domains] take the form of technology, rules and rituals."[132] *Individualism*, in contrast to *collectivism*, is identified as "the relationship between the individual and the collectivity that prevails in a given society [and is] reflected in the way people live togetherâÄ"for example, in nuclear families, extended families, or tribes."[133] *Masculinity/femininity* refers to the implications of biological sex "for the emotional and social roles of the genders" in a society.[134] Finally, *long-term orientation* cultures are characterized as ones that "place more importance on values associated with future orientation, while *short-term orientation* cultures place more importance on values associated with past and present orientation."[135]
The following discussion summarizes the results of Hofstede's research regarding differences that emerged in the five dimensions of culture for U.S., British and Indian workers, despite English as a commonly-shared language.[136]

- Indian employees scored significantly higher in acceptance of *power distance* than British and U.S. employees.
  - Workers in countries that score high in *power distance* generally honor the decisions of their superiors, and are less likely to question authority or the ethicality of management decisions.[137] Companies in these countries tend to utilize more centralized decision structures, more concentrations of authority, and more supervisory personnel.[138] Managers tend to rely on normal rules and authoritative leadership styles.[139] To their detriment, high power-distance countries more often experience sudden changes in government due to revolution or instability, increased corruption, and expectations that scandals will be covered up.[140]

- British and Indian employees scored lower on *uncertainty avoidance* than U.S. employees, although all three countries scored in the low-to-moderate range.
  - People from countries that score low on *uncertainty avoidance* tend to have a higher "tolerance for ambiguity in structures and procedures" and a "belief in common sense."[141] Additionally, they are trustworthy, more likely to take risks or break rules (if necessary), and less likely to see company loyalty as "a virtue."[142]
- Indian employees exhibited less *masculine* (i.e., competitive) tendencies than employees from the U.S. and Britain.
  - Employees from countries that score lower in *masculinity* (or higher in *femininity*) tend to be cooperative at work and to view the superior-subordinate relationship as important.[143] Problem solving, compromise, and negotiation are preferred strategies to solve problems, which gives these cultures "a competitive edge in the service industries."[144]
- U.S. and British employees scored significantly higher in *individualism* than Indian employees. In fact, U.S. employees "set the bar" on this cultural dimension.
  - Countries that score lower in *individualism* (or higher in collectivism) produce workers that have strong family ties, experience little personal privacy, and see "trespassing" as a reason to feel shame and lose face.[145] They tend to have high "moral involvement" with their companies, [146] perceive their identities through the lens of their social systems,[147] and act in the interest of the group rather than in their own self-interests.[148] In fact, "placing individual over collective interests [may be perceived] as evil." [149] As a result, their private lives are often "invaded by public interests, and their opinions and votes [may be] predetermined by in-group membership."[150]
- Indian employees scored higher in *long-term orientation* than U.S. and British employees.
  - Individuals from countries that score high in *long-term orientation* are generally able to "adapt their traditions to new circumstances" and see the most important events in their lives as happening in the future.[151] If they are religiously devout, they may believe in the importance of ethical principles, a detached attitude toward life, and deferred gratification of needs.[152] Perceptions of what is good versus evil may "depend on the circumstances."[153]

2. THE RELATIONSHIP BETWEEN HOFSTEDE'S DIMENSIONS OF NATIONAL CULTURE, PERCEPTIONS OF DATA PRIVACY, AND INTERNATIONAL REGULATORY MODELS

In 1995, Milberg, Burke, Smith, and Kallman identified five international regulatory models regarding information privacy, based on a continuum of government involvement in day-to-day corporate privacy management: the (1) *Self-help*, (2) *Voluntary Control*, (3) *Data Commissioner*, (4) *Registration*, and (5) *Licensing* models. At the low end of the continuum, anchored by the Self-help Model, "government assumes a 'hands-off' role and allows corporations to monitor themselves, with reliance on injured individuals to pursue their own remedies in the court system."[154] At the high end, anchored by the Licensing Model, "government assumes the authority to license and regulate all corporate uses of personal data, including the right to conduct inspections inside corporations and to examine all proposed applications of personal data before they are implemented."[155]
Based on this continuum - and the work of Westin in 1967, [156] which found that expressions of privacy vary significantly across cultures - Milberg and her colleagues proposed and tested a theoretical model of the relationships among nationality, cultural values, level of information privacy concerns, and regulatory approaches.[157] Overall, their study revealed significant statistical relationships between (1) nationality and information privacy concerns, and (2) information privacy concerns and privacy regulations. As the researchers noted, "countries with either 'no privacy regulation,' or the most strict model of privacy regulation (registration model) were associated with significantly lower information privacy concerns than those using the other three models. Countries with more moderate regulatory structures were associated with higher aggregate levels of concern, and those levels of concern were not significantly different from one another."[158]
Although India was not included in this initial study, the U.S. and three E.U. countries (France, Denmark, and U.K.) were included. Regarding these specific nations, Milberg and her colleagues found that the regulatory models of the U.S. and three E.U. Member States reflected moderate regulatory structures with varying levels of aggregate concern. France was associated with the least strict of the regulatory models, the Self-Help Model, and Denmark and the U.K. were allied with the more stringent Registration Model. The U.S. was associated with the Voluntary Control Model, with regulation driven primarily by U.S. companies.[159]
In 2000, Milberg, Smith, and Burke revised and extended their model from the original four variables (i.e., nationality, cultural values, information privacy concerns, and regulatory approaches) to include the following six variables: (1) cultural values, (2) individual privacy concerns, (3) regulatory approaches, (4) corporate privacy management environment, (5) privacy problems, and (6) regulatory preferences.[160] To assess the efficacy of their revised model, the authors tested (and partially confirmed eight of) nine hypotheses regarding the interrelationships among these variables. Additionally, the researchers revised and extended their original country classifications by regulatory model. Pertinent to the present discussion are the authors' revised country classifications, which placed India in the category of "no formal information privacy regulation, and the U.S., once again, in the "voluntary control" classification. Eight E.U. nations were categorized by the researchers, as follows: Italy was added to the "no formal information privacy regulation" category; Finland and Germany were identified as reflecting the "data commissioner" model; Belgium,

Denmark, France, Netherlands, and Great Britain were associated with the "registration" model; and no countries were classified as adhering to the "licensing" model.[161] The researchers' general conclusions associated with this study also are relevant for U.S. and E.U. companies that outsource to India and for Indian BPO providers. These conclusions were succinctly presented in the discussion section of their study:

A country's cultural values are associated strongly with the privacy concerns that are exhibited by its populace (Hypothesis 1) and are associated marginally with its regulatory approach (Hypothesis 2). As information privacy concerns rise and governments become more involved in corporate privacy management, management of privacy seems to tighten (Hypotheses 3 and 4 respectively) and, in turn, fewer specific privacy problems are reported (Hypothesis 5). Moreover if corporations exhibit loose management of information privacy, then individuals are more likely to call for strong privacy laws rather than allowing corporations to self-regulate (Hypothesis 6). Similarly, as individuals' privacy concerns rise, so do their demands for additional legal intervention (Hypothesis 8). There is also a marginal, positive association between the level of governmental involvement in corporate privacy management and respondents' preferences for strong laws (Hypothesis 9). The single hypothesis that received no support in this study (Hypothesis 7) was an *exploratory* one that predicted that, as respondents perceived larger numbers of areas in which there were corporate privacy problems, they would call for stronger law as a remedy and be disinclined to rely on corporate regulation. In fact, a much stronger predictor of regulatory preferences appears to be the manner in which corporations manage their privacy environment "via their policies and structures" rather than specific privacy problems that may be observed.[162]

C. LEGAL AND POLITICAL INTERPRETATION OF THE RESEARCH ON DATA PRIVACY AND REGULATORY MODELS: THEORY MEETS PRACTICE

Hofstede's theory, as well as subsequent research by Milberg and her associates, can be used to explain the emergence of (1) current international initiatives, (2) the E. U. omnibus approach, (3) the U.S. sector approach to data privacy protection, and (4) India's slow progression toward legislation protecting data privacy. The following discussion addresses these four subjects and interprets them in light of important historical and political factors.

1. INTERNATIONAL INITIATIVES

Although there was some recognition by the United Nations of the right to privacy as early as 1948, the modern history of data privacy protection began in the 1960s and 1970s with the growth of the information technology industries.[163] Many of these European laws, as well as those enacted in other nations, are based on two important international documents emanating from the Organization for Economic Cooperation and Development ("OECD") and the Council of Europe.[164]

The OECD was the first to adopt a document in 1980.[165] The OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data are a set of non-binding rules for handling electronic data signed by OECD members, including the U.S.[166] The OECD Privacy Guidelines have been widely used in national legislation, even outside the OECD countries.[167]

In 1981, the Council of Europe adopted the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, which established privacy as a human right in Europe.[168] The rules in the OECD and Council of Europe documents form the core of data protection laws in dozens of countries, as well as the E.U. Both documents call for privacy protection legislation, [169] encourage the flow of data among member nations, [170] and support restrictions on the transborder transfer of data if the recipient country fails to provide a sufficient level of data protection.[171] These components are reflected in the E.U. Directive that was issued almost fifteen years later, although the E.U. Directive further expands protection privacy guidelines.

In 2005, the International Standards Organization "ISO") adopted a best practices code for information security.[172] The code establishes a certification standard. Certificates can be issued against the standard by accredited certification bodies. Two sections of ISO/IEC 17999 are particularly relevant. The first section, "Protect the privacy of personal information" recommends: (1) compliance with all relevant legislation related to the use of personal data, and (2) the appointment of a data protection officer to provide advice on personal data issues.[173] The second section, "Prevent misuse of data processing facilities" recommends that companies: (1) ensure that data processing facilities are not used for non-business purposes, and (2) that companies monitor the use of data processing facilities to detect unauthorized use.[174] Additional recommendations are offered for implementing a suitable set of controls that ensure a quick, effective and orderly response to security incidents,[175] with a report to management as soon as possible.[176]

2. EUROPEAN UNION OMNIBUS APPROACH

The European legal regime's *omnibus* (comprehensive) approach to data protection is rooted in their cultural belief that data privacy is a fundamental human right. In fact, their distrust is so deeply rooted that the right to personal data privacy is in the constitutions of many European countries.[177] As a result, data protection laws exist in Europe to protect private citizens and to ensure that personal data are not processed in ways that infringe upon an individual's right to privacy.[178] Although this approach to privacy has deep roots in the civil law tradition, it is likely that the development of modern data privacy laws was fueled by the uses made of personal data by Germany and the repressive regimes in countries that are now E.U. Member States.[179] These abuses logically form the basis for the modern European view of privacy.[180] Data protection laws became the essential means to protect that right.[181] Thus, it is understandable that Europeans weigh the right to privacy against the right of public access to information much differently than Americans. In Europe, information about a person is believed to belong to that individual, and personal information is treated as intellectual property.[182] This approach is unlike the U.S approach, and the differences manifest themselves in fundamentally different laws and regulation.

3. UNITED STATES SECTOR APPROACH

In contrast to the E.U., the U.S. has adopted a *sector* (rather than a comprehensive) approach to data privacy, which is rooted in the culture's deeply held belief in freedom of speech (i.e., the free flow of information) and perceived as more important than individual privacy rights. The government is limited in terms of how it can treat personal information, but private industry has few such restrictions. This fact reflects Americans' fundamental distrust of government intervention into the private sphere. Consequently, there is no omnibus federal data privacy law. Instead, the privacy laws are embodied in separate federal legislative enactments discussed supra: the Fair Credit Reporting Act,[183] the Gramm-Leach-Bliley Act[184], the Health Insurance Portability and Accountability Act,[185] and the Sarbanes-Oxley Act.[186] As Milberg and her colleagues confirmed, Americans prefer a regime of industry self-regulation without significant government intervention.[187] Americans' ongoing distrust of government intervention has created a socio-political environment resulting in Congress rejecting most attempts to pass comprehensive legislation related to the treatment of personal data by individuals and businesses in the private sector.[188] However, there is strict regulation of government entities' treatment of personal data.

4. INDIA: ABSENCE OF DATA PRIVACY REGULATION

India has approached the adoption of data privacy laws very reluctantly. By late 2005, India had still not adopted legislation governing the protection of personal data. Although data privacy protection was discussed in the late 1990s as part of the formal discussions regarding the provisions to be included in the pending IT Act, the final version of the IT Act of 2000 did not include data privacy.[189] Recommendations have been made to amend the IT Act of 2000 by including data privacy protection, but steps toward doing so have been slow as evidenced by the reports over the last several years about pending action by the Indian legislature.[190] The current solution to the problem is still for Indian companies to institute their own security measures. However, the recent highly publicized incidents of misuse of private data by service provider employees threaten millions of dollars of revenue for Indian companies and may provide the impetus for legislative action.

India has several reasons for not rushing into the drafting and adoption of data privacy laws: (1) their history is not

embedded with abuses of privacy; (2) no serious resentment exists toward a centralized government; (3) privacy is not an issue with a population density of approximately 1.1 billion people in a geographic area one-third the size of the U.S.; and (4) problems of identity theft are not prevalent in India. At the time of this writing, there are no national identity card numbers, no social security numbers, few driver's licenses (as middle and upper class people usually have drivers), and few PINS for bank accounts (because bank usage is not prevalent among the lower echelons of Indian society).

Another possible reason for the reluctance of the Indian legislature to hurriedly respond to the need for adoption of data privacy protection may be a deeply rooted skepticism of the government's ability to efficiently handle implementation of the law. The causes for the skepticism can be traced to 1947 when India received its independence from Great Britain.[191] Although India had a democratic form of government, it chose a socialist economic path that resulted in an obstructive bureaucracy.[192] Without infusion of the respect for private business and the profit characteristics of capitalism, India engaged in relentless overregulation.[193]

Congress Party's Jawharlal Nehru, who dominated the political scene in India from 1947 until his death in 1964, thought competition was wasteful.[194] The country followed the pattern of distrust established by the British Raj[195] that resulted in an almost impossible array of rules and regulations that had to be followed.[196] In the wake of this pattern, businesses in the private sector had to wait months or years for a response to their requests for government approvals of entrepreneurial projects âÄ" many times waiting in vain.[197] To exacerbate the situation, Indian civil service workers were underpaid, and bribes were extracted from businesses seeking government permits and services.[198] The name "License Raj" was given to the unwieldy and sometimes ludicrous burden of government controls.[199]

Two major legislative statutes, enacted under Prime Minister Indira Gandhi, further stifled Indian businesses: the Monopolies and Restrictive Trade Practices Act in 1969[200] and the Foreign Exchange and Regulation Act of 1973.[201] In the late 1980s Prime Minister Rajiv Gandhi recognized the advantages of private enterprise and become alert to the new world of computers and mobile capital.[202] As discussed supra, it was during this period that General Electric's CEO, Jack Welch, met with Rajiv Gandhi and began GE's outsourcing of business functions to India.[203] The first major emergence of private business from the morass of excessive government control came in 1991 when Finance Minister Manmohan Singh, under Prime Minister Rao, began dismantling the massive system of government regulation and eliminating the trade side of the License-Permit Raj.[204] The repressive environment, in which private businesses operated for forty years during the years after the end of British colonization of India, has caused an understandable fear of the return of License-Permit Raj.

However, despite the social, historical and political reasons for Indian business people to approach regulation of data protection with skepticism, a number of other factors make it necessary for that skepticism to be set aside and to make data privacy protection a priority, including: (1) the growing contribution of business process outsourcing to the nation's economy; (2) the need by Indian outsourcing firms to meet the "adequacy" standard of the E.U. Directive;[205] and (3) the importance of quieting the nerves of U.S. businesses driven by their American customers and clients who have heard about the data privacy breaches that have occurred in India, and are jittery because of recent occurrences of identity theft in the U.S..[206]

VII. RECOMMENDATIONS

In this section, the authors offer lists of recommendations regarding the protection of data privacy at the international, national, and company levels:

A. LIST OF RECOMMENDATIONS AT THE INTERNATIONAL LEVEL

· An international summit, where major policy makers from the leading countries involved in transborder data flow can openly debate such topics as:
· Merits of the omnibus versus the sector approach to data privacy protection.
· Socio-cultural issues related to data privacy protection.[207]
· National security and sovereignty issues.[208]
· Economic issues.[209]
· Innovative legal structures and solutions.
· Methods for establishing an effective legal framework to provide adequate protection of nonpublic personal information.
· The creation of a formal organization of the top information privacy officials from around the world patterned along the same lines as the International Organization of Securities Commissioners.

Two possible outcomes could arise from such debates: (1) development of a permanent monitoring system to address political, social, economic, and legal conditions that threaten to place personal data privacy at risk; and (2) innovative legislative and policy solutions that could be agreed upon and adopted worldwide.

B. LIST OF RECOMMENDATIONS AT THE NATIONAL LEVEL IN THE U.S.

· Adopt federal legislation that mirrors the California Mandatory Disclosure law, which requires an organization to inform its customers if any of their personal data are compromised as a result of a security breach.[210]
· As recommended in a bill introduced by Senator Clinton in 2004, adopt legislation similar to the E.U. Directive, which mandates that "if a company wishes to transfer personally identifiable data regarding a U.S. citizen to any foreign affiliate or subcontractor, it may only do [so] if the receiving company is located in a jurisdiction that provides adequate protection."[211]

C. LIST OF RECOMMENDATIONS AT THE NATIONAL LEVEL IN INDIA

· Pass the amendments to the existing IT Act, 2000, which were recommended by NASSCOM and the Indian Ministry of Technology, or (to act more expeditiously) issuance of an Executive Order.[212]
· Obtain E.U. approval of Safe Harbor Principles that meet the "adequacy" requirement of the E.U. Data Privacy Directive.
· Examine the laws and regulations of the countries or regions with which they do outsourcing business, and development of international initiatives for data privacy laws based on a Western model to maintain the level of confidence now enjoyed by Indian companies.
▪ Reference the OECD Privacy Guidelines and the Council of Europe Convention as models for a data privacy law.

D. LIST OF RECOMMENDATIONS AT THE COMPANY LEVEL

· Incorporate the following contractual provisions between U.S. companies and India BPO service providers:
· A requirement for the adoption of the international standards of best practices of ISO/IEC 17799[213] (and BS 7799[214]) on data privacy and *an assessment by an accredited third-party certification body against BS 7799*.[215] (All participating businesses should be certified/accredited.)
· An international arbitration provision for dispute resolution, which covers at a minimum, the scope of arbitration; arbitration institution;[216] and choice of law, forum, and language.[217]

· An obligation for mandatory training of all employees regarding legal and ethical conduct.
· A stipulation requiring insurance to cover liabilities that may arise from potential law suits.
· Mandatory adoption of multilayered encryption/decryption techniques to deny employees direct knowledge of customer data.
· A requisite for the signing of nondisclosure agreements by employees.

VIII. CONCLUSION

Despite the harsh criticism of offshore outsourcing in the U.S., companies will continue to take economic advantage of business process outsourcing in our globalized society. Barring any major, unforeseen events, we can expect U.S. businesses to increase the offshoring of business process and information technology functions to India. Regardless of its overwhelming infrastructure and overpopulation problems, India provides a conducive business environment for U.S. companies because the country has adopted a stable, secular democracy, and offers low-cost labor and world-class managerial talent capable of adapting to western culture and language. Since the trend of business process outsourcing is to increase transborder data flows, it is incumbent upon legislators, regulators, non-governmental organizations, privacy advocates, and U.S. companies to ensure that the BPO relationship with India is established so all of the safeguards for data privacy are established.
At this time, the primary protection against the possibility of catastrophic breaches of personal data privacy is limited to the unique positive cultural traits of the Indian people[218] and fiercely competitive market forces.[219] Indian BPO providers have a lot at stake because they must remain economically viable against the challenges of competition from the Philippines, Latin America, Eastern Europe and China.[220] As one discerning Indian industry source has noted, "All it takes is one major incident of identity theft or leakage of sensitive data for trust built up over years to collapse."[221] Although a recognition that any major leak of sensitive information could destroy their competitive position is a powerful market incentive for Indian companies, this same recognition should be a basis for driving enlightened debate in India regarding appropriate regulatory or legislative action.

APPENDIX A: Examples of The Legislation, Regulations, and Self-Regulation The United States Relies On For Data Protection

The primary federal laws are:
§ The Fair Credit Reporting Act (FCRA) [222] passed by Congress during the height of the consumer movement in the 1960s and early 1970s, along with a series of laws that supported basic consumer rights. The FCRA applies to private sector credit reporting agencies and gives consumers the right of access to personal information held by a third party so that consumers can identify information that negatively affects their credit ratings.[223]
§ The Health Insurance Portability and Accountability Act (HIPAA) passed in 1996, which requires consumer consent before companies share medical data.[224]
§ The Financial Services Modernization Act (Gramm-Leach-Bliley Act or GLBA) passed in 1999, which imposes the affirmative obligation in § 501(a) that a financial institution must respect the privacy of its customers and protect the security and confidentiality of customers' nonpublic personal information.[225] Under 501(b), regulators of federal financial institutions are directed to establish standards for financial institutions relating to the administrative, technical and physical safeguards of that information in order to (1) ensure the security and confidentiality of customer information, (2) protect against any anticipated threats or hazards to the security or integrity of such information, and (3) protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.[226]
§ The Sarbanes-Oxley Act (SOX), which became effective in July 2002 in response to the massive accounting fraud uncovered in many large U.S. corporations.[227] SOX affects corporate governance, financial disclosure and the practice of public accounting. The legislation extends beyond the accounting functions of a company to "allow it to develop a broader-based incident response system to meet the requirements of other laws and regulations" and to include a tightening of data controls. [228]
Examples of regulatory agency action are as follows:
§ Under the implementing rules of §404 of SOX, the Securities and Exchange Commission (SEC) requires internal control procedures that provide reasonable assurance regarding "prevention or untimely detection of unauthorized acquisition, use or disposition of the assets that could have a material effect on the financial statements."[229]
§ On December 20, 2000, the U.S. Department of Health and Human Services issued standards for protecting the privacy of Americans' health records under HIPAA.[230] The standards require that documenting, reporting and responding to data privacy breaches be included as an integral part of a security program.[231] Furthermore, the issuance of federal privacy regulations effective in 2003 require written contracts with third-party business associates and impose various obligations regarding protected health information.[232]
§ The Federal Trade Commission (FTC) is one of eight federal agencies that are responsible for administering and enforcing the Financial Privacy Rule to meet one of the requirements of Gramm-Leach-Bliley.[233] The rule applies to protection of nonpublic personal information[234] and requires financial institutions to give their customers privacy notices that explain the financial institution's information collection and sharing practices.[235] The FTC also issued a Safeguards Rule under the authority of Gramm-Leach-Bliley, entitled "Standards for Insuring the Security, Confidentiality, Integrity, and Protection of Customer Records and Information."[236]
§ The Treasury Department maintains Safety and Soundness security guidelines that specifically require banks to implement "response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies."[237]
§ Under the Gramm-Leach-Bliley Act, regulatory agencies such as the FTC, the Office of the Comptroller of the Currency, and the Federal Insurance Corporation have the power to enforce GLBA with fines and injunctive relief.[238]
Using California as a model, some relevant data privacy protection laws
are as follows:
§ On January 1, 2005, California legislation (AB 1950) became effective and requires a business that owns or licenses personal information about a California resident to: a) implement and maintain reasonable security procedures and practices appropriate to the nature of the information, and b) protect personal information from unauthorized access, destruction, use, modification, or disclosure.[239] Furthermore, "a business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[240] Personal information includes social security numbers, driver's license numbers, account numbers, credit card or debit card numbers (in combination with any required security codes, access codes, or passwords), and medical information.[241]
§ On July 1, 2003, California's Mandatory Disclosure Law (SB 1386) became effective.[242] This law requires an organization to inform its customers if any of their personal data are compromised as a result of a security breach.[243] The law applies to "any person or business that conducts business in California" and requires them to notify California residents whose "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[244] Personal information is defined in the statute as an individual's name in combination with any one or more of the following: social security number, driver's license number, bank account numbers, credit card or debit card numbers, together with any required security codes, access codes or passwords permitting access to the individual's financial account.[245]

---

[1] Forbes.com, India Controls 44 Percent of Outsourcing (June 12, 2005), http://nasscom.org/artdisplay.asp?Art_id=4406 (reporting for the main infotech trade body that revenues for Indian companies reached US$17.2 billion in the year ended March 2005). *See also* Neil King Jr., *A Whole New World*, Wall St. J., Sept. 27, 2004, at R3 ("Rafiq

Dossani of Stanford University and Martin Kenney of the University of California at Davis predict that India will have more than 500,000 people working in back-office, or 'business process,' jobs by 2006, up fivefold in less than four years.").
[2] Jordan Rau, *Offshore Jobs Bill is OKd,* L.A. Times, Aug. 24, 2004, at B1. Companies use India-based independent firms or their own Indian units. Wages paid in India are approximately 1/5 of those paid in the U.S.
[3] *See* Saritha Rai, *In India, Outsourcing Firms Rejoice,* Int'l Herald Trib. Nov. 5, 2004, at 1. *See also* Chidanand Rajghatta, *Bush Blesses Outsourcing to India,* The Times of India, Feb. 10, 2004, *available at* http://timesofindia.indiatimes.com/articles show/488790.cms.
[4] Cal. Civ. Code §1798.81.5(b-d)(1) (West 2006) (Requiring companies to maintain reasonable security procedures and defining personal information as: an individual's name in combination with any one or more of the following: social security number, driver's license number, account number, credit card or debit card number, together with any required security code, access code or password permitting access to the individual's financial account, medical information).
[5] *See* Editorial, *Data Protection, Post-Haste*, Econ. Times, Jan. 3, 2005, available at http://economictimes.indiatimes.com/articlesho w/978632.cms. "A survey done by [the National Association of Software and Service Companies] NASSCOM in association with [its American counterpart] the Information Technology Association of America reportedly revealed that security was a key concern of the customers of 76% of the companies surveyed." *See also* Federal Deposit Insurance Corporation, *Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks*, June 2004, http://www.fdic.gov/regulations/examinations/offshore/ [hereinafter Offshore Outsourcing of Data Services by Insured Institutions].
[6] Michael Fitzgerald, *At Risk Offshore,* CIO Mag., Nov. 15, 2003.
[7] *See* Harbaksh Singh Nanda, *India's Cyber Law Feels Heat of Porn Clip,* United Press Int'l Jan. 10, 2005, *available at* http://www.washtimes.com/upi-breaking/200 50110-122739-8232r.htm. (Pavan Duggal, India's leading cyber law expert, has argued for amended legislation because the "IT Act, 2000 lacked the necessary teeth to deal with the growing number of cyber crimes.")
[8] The offshore business process outsourcing (BPO) refers to the relocation of business processing to lower-cost offshore centers. Organizations have been able to relocate existing jobs almost unchanged to lower cost locations, reusing existing applications and systems. Organizations can either set up their own offshore processing center to access these resources, or to make use of a local third party provider to set-up and run the process on an outsourced basis. *See BPO and Relocation: Where Next?* Back Office Focus, May 2003.
[9] Directive 95/46/EC, Protection of Individuals with Regard to the Processing of Personal Data on the Free Movement of Such Data, 1995 O.J. (L281) 31, *available at* http://www.cdt.org/privacy/eudirective/EU_Directive_.html#HD_NM_42. [hereinafter, the Directive] Participation in the "Safe Harbor" creates a presumption that a company provides an adequate level of privacy protection and qualifies the company to receive data fro E.U. Member States.
[10] *Id.* Art. 25 § 4
[11] The sector-specific approach used in the U.S. is reflected in its adoption of the Fair Credit Reporting Act, 15 U.S.C. § 1681 (regulates the collection and use of credit information).
[12] Issuance of Safe Harbor Principles and Transmission to European Commission; Procedures and Start Date for Safe Harbor List, 65 Fed. Reg. 56,534 (Sept. 19, 2000).
[13] Charles D. Raab, Colin J. Bennett, Robert M. Gellman & Nigel Waters, *European Commission Tender No. XV/97/18/D, Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals with Regard to Processing Personal Data: Test of the Method on Several Categories of Transfer*,202 (1998), *available at* http://europa.eu.int/comm/justice_home/fsj/privacy/docs/studies/adequat_en.pdf..
[14] Aziz Haniffa, I am a big fan of Manmohan Singh: Jack Welsh, India Abroad, May 20, 2005, at A30, *available at* http://us.rediff.com/money/2005/may/21binter.htm. *See also* Jay Solomon & Kathryn Kranhold, *In India Outsourcing Boom, GE Played a Starring Role,* Wall St. J., Mar. 23, 2005, at A1.
[15] Jay Solomon & Kathryn Kranhold, *In India Outsourcing Boom, GE Played a Starring Role,* Wall St. J., Mar. 23, 2005, at A1.
[16] Thomas L. Friedman, The World is Flat 106 (Farrar, Straus and Giroux 2005).
[17] Solomon *supra* note 16.
[18] A small group worked on dismantling the controls applicable to thousand of products that were set forth in the infamous Red Book, all of which and more were agreed to and augmented by Finance Minister Singh with the backing of Prime Minister Rao. Gurcharan Das, India Unbound 216-218 (Anchor Books, 2002) . *See also* Friedman, *supra* note 17, at 107.
[19] Friedman, *supra* note 17, at 107.
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] Jack Welch with John A. Byrne , Jack, Straight From The Gut 309 (Warner Books 2001).
[24] Friedman, *supra* note 17, at 109.
[25] Although Hindi is the national language and the primary language of 30% of the Indian people, the English language has been granted associate status. *See* World Fact Book, *at* http://www.cia.gov/cia/publications/factbook/goes/in.html#Intro (last visited Jan. 10, 2006).
[26] Friedman, *supra* note 17, at 111.
Id.
[28] *Id.* at 109. In making the keynote address at the TiEcon 2005 Conference in May 2005 at Santa Clara, California, Thomas Friedman stated, "With the laying of that fiber optic cable, Bangalore, Beijing, Boston and Silicon Valley all become next door neighbors." *See Learn how to learn, says Friedman, India Abroad,* May 27, 2005, at A33.
[29] It is estimated that there are 300 million in India who fall into the category of "middle class."*See Ben Wattenberg Think Tank,* Interview with Thomas L. Friedman on the future of globalization (Part 1 of 2), KCET public broadcasting station, Los Angeles, CA, (June 25, 2005) [hereinafter Interview with Thomas L. Friedman].
[30] Todd Furniss and Michel Janssen, *Offshore Outsourcing Part1: The Brand of India,* April 2003, *available at* http://www.bpo-outsourcing-journal.com.
[31] Shekhar Gupta, editor of The Indian Express as quoted in Thomas L. Friedman *35-hour week? 35-hour day!*, Int'l Herald Trib, June 4-5, 2005, at 7.
[32] *See* Saritha Rai, *An Industry in India Cheers Bush's Victory,* N.Y Times.com, Nov. 4, 2004, LEXIS.
[33] *See* Siddharth Srivastava*, Call Center Scandal, Security Breach in Indian BPO,* Siliconeer, Sept. 2005 at 6. *See also id.*.
[34] India's Silicon Valley, *available at* http:/www.businessweek.com/adsections.indian/infotech/2001/silicon.html (last visited April 2, 2006). The city of Bangalore boasts that dozens of multinational corporations have offices there, along with the major Indian information technology and service companies. Bangalore is linked up with a satellite and is wired to the world with thousands of miles of fiber optic cable. Located in a region with a mild climate in the center of southern India, it is a city that is ready, willing and able to meet the outsourcing needs of companies around the world. Friedman, *supra* note 17, at 109, 110. However, it is a city with a population of 7 million that has not solved all of its infrastructure problems that are inherent in a developing country that has 1/3 the land space of the U.S. and 3-1/2 times the population of the U.S.
[35] Rai, *supra* note 33.
[36] David Streitfeld, *Kerry's Plan to Rein in Outsourcing Has Holes,* L.A. Times, Oct. 8, 2004, at A1.
[37].Rai, *supra* note 33.
[38] Chidanand Rajghatta, *Bush Blesses Outsourcing to India,* Times News Network, Feb. 10, 2005, LEXIS.
[39] *Id.*
[40] Jyoti Thottam, *Is Your Job Going Abroad,* Time, Feb. 23, 2004.
[41] Congressman Edward J. Markey, senior Democrat on the Telecommunications and Internet Subcommittee and co-chair of the Privacy Caucus, sent letters in Feb. 2004, to several federal and state agencies raising the privacy issue and alleging that off-shoring represented a risk not only to American jobs but also to privacy.
[42] Joseph Menn, *Hackers Tap 40 Million Credit Cards,* L. A. Times, June 18, 2005, at 1.
[43] Bill Saporito, *Are Your Secrets Safe?* Time, March 7, 2005, at 46. Intruders posing as small-business customers tapped personal data on as many as 145,000 people. *See* Jonathan Peterson, *U.S. Senate Panel Tackles Identity Theft,*

L.A. Times, March. 11, 2005, at C1.
[44] *Id.* Bank of America lost five computer tapes containing personal information on federal employees who used 1.2 million bank-issued cards.
[45] *See* Tom Zeller Jr., *Sensitive Data Slip Out,* Int'l Herald Trib., June 10, 2005, at 15. A magnetic tape with information on about 120,000 Japanese customers disappeared while being shipped by truck from a data management center in Singapore. The tape held names, addresses, account numbers and balances.
[46] *See* Clint Sett, *Senators Target Outsourcing of Jobs,* Sacramento Bee, March 10, 2004, at D1. Salary comparisons indicate that in the U.S. an accountant will receive an average annual salary of $41,000 while in India, the annual average salary is $5000. *See America and Jobs,* Forrester Research, Inc, Nov. 2002*, available at* http://www.pbs.org/now/politics/utsource.html.
[47] Outsourcing Journal, Legal Voice - International Disputes, *available at* http://www.outsourcing-journal.com/aug2000-legal.ht ml (last visited Apr. 15, 2006).
[48] Nikki Swartz, *Offshoring Privacy,* Info. Mgt. J., Sept/Oct. 2004, *available at* http://www.find articls.com/p/articles/mi_qa3937/is_200409/ai_n9452822 (last visited July 1, 2005).
[49] Jason Overdorf, *Unclogging the Courts, The Indian justice system is legendary for its delays and diversions. But changes are finally on the way,* Newswk, July 18, 2005, *available at* http://www.msnbc.msn.com/id/85525757/site/newsweek/from/RL.2/.
[50] *British Tabloid's Sting has BPOs Hurting over Privacy Violation,* Fin. Times Information, June 24, 2005, LEXIS.
[51] *Id*
[52] *London Police Called into Call Centre Fraud, available at* htttp:sify.com/finance/full story.php?id+13880402 (last visited June 25, 2005).
[53] Pavan Duggal, Law of Business Process Outsourcing 8 (Saakshar Law Publications 2004)..
[54] *Indian Workers Resist Unions,* L.A. Times, Sept. 24, 2005, at C8.
[55] As a basis of comparison, the per capita income in India is $470 while the per capita income in the U.S. is $35,000 a year. *See* Interview with Thomas L. Friedman, *supra* note 30.
[56] . *London Police Probe into Call Centre Fraud,* June 24, 2005, *available at* http://sify.com/finance/fullstory.php?id=13880402.
[57] *Nasscom Takes Note of Security Breach,* June 24, 2005, *available at* http://sify.com/finance/fullstory.php?id=13880354.< /p>
See 12 Accused of Using Call Center in India to Cheat Citibank Clients, N.Y. Times, Apr. 9, LEXIS. *See also* Josey Puliyenthuruthel and David Rocks, *The Soft Underbelly of Offshoring,* Bus. Wk. Online *available at* http://www.businessweek.com (Apr. 25, 2005).
[59] *Id.*
[60] *Offshoring and Privacy Protection,*Public Citizen, http://www.citizen.org/trade/offshoring/privacy/index.cfm (last visited May 10, 2005).
[61] Gaurav Bhagowati, *India Responds to Growing Concerns Over Data Security,* Outsourcing Center, Dec. 2004, *available at Outsourcing-best-practices.com/security.html* (last visited July 1, 2005).
[62] Nikki Swartz, *Offshoring Privacy,* Info. Mgt. J., Sept./Oct. 2004, *available at* http://www.find articls.com/p/articles/mi_qa3937/is_200409/ai_n9452822.
[63] Srivasyava, *supra* note 34.
[64] Engardio, Pete and Majeet Kripalani and Josey Puliyenthurrthel, *Fortress India?,* Bus. Week, Aug. 16, 2004, at 1.
[65] Bhagowati, *supra* note 62.
[66] Engardio et. al, *supra* note 54.
[67] *Id.*
[68] *Id.*
[69] *Boomtown Blues, India Abroad,* July 8,2005, *at* A20.
[70] Bhagowati, *supra* note 62.
[71] Special training includes the basics of cyber-crime, including how to trace an offending internet user's computer IP address and how to extract and store electronic evidence from a computer hard drive. The cyberlaw sections within police departments have trained investigators who focus solely on computer crimes. *See NASSCOM to Hold Two-Day Security Summit in Delhi,* , Asia Pulse Pte Limited, Oct. 5, 2004, LEXIS; James Jay Carafano & Paul Rosenzweig, *Protecting Privacy and Providing Security: A Case of Sensible Outsourcing,* Nov. 5, 2004, *available at* http://www.heritage.org/Research/HomelandDefense/bg1810.cfm .
[72] Edward Luce, *India Acts to Protect Call Center Security,* Fin. Times, Oct. 14, 2004, LEXIS.
[73] *Id. See also* Srivastava, *supra* note 34.
[74] Srivastava, *supra* note 34.
[75] Karl Schoenberger, *Outsource Firm Sues in India: Alleged Code Theft Highlights Foreign Risk,* Nov. 30, 2004,*available at* http://www.siliconvalley.com/mld/si.
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] Offshore Outsourcing Center, OOC.com/blog/archives/2004/09 (last visited July 13, 2005)
[80] Since its inception in Berlin in 1993, Transparency International (TI) has been exclusively devoted to curbing corruption. One of TI's most widely publicized activities has been its annual survey ranking countries based on their perceived level of bribe taking, the TI Corruption Index. The Index has become an internationally acknowledged instrument for measuring corrupt practices, as perceived by business people.
[81] *See* Transparency Int'l, 2004 *Corruption Index,* http://ww1./transparency.org/cpi/20005/cpi20 005_infocus.html (last visited April 1, 2006).
[82] *IISc Gunman Nabbed in Chennai,* Deccan Herald, Jan. 6, 2006, at 1.
[83] Offshore Outsourcing of Data Services by Insured Institutions, *supra* note 5, at 16.
[84] Nanda, *supra* note 7.
[85] Wipro, one of India's largest companies engaged in outsourcing, was built from a $150 million software-services provider in 1999 to the current $1.4 billion powerhouse whose 41,000 employees offer a range of tech and back-office services. *See* Manjeet Kripalani & Steve Hamm, *Leaving a Vacuum at Wipro,* Bus. Wk., July 11, 2005, at 52.
[86] *British Tabloid's Sting has BPOs Hurting over Privacy Violation, supra* note 51.
[87] Directive, *supra* note 10.
[88] *Id.*, at art. 1.1.
[89] Id, at art. 25.1.
[90] *See* Sridhar Balaji, *Plan for Data Protection Rules when Moving IT Work Offshore,* Computer Wkly, Nov. 26, 2004, LEXIS
[91]. *Id.*
[92] There are seven Safe Harbor Principles: Notice, Choice, Onward Transfer, Access, Security, Data Integrity, and Enforcement.
[93] Simon Chester, *Outsourcing Threat to Privacy Overblown,* Aug. 16, 2004 LEXIS, Financial Post.
[94] Directive, *supra* note 10, at art. 25, 26.
[95] *Id.*, at art. 25.4.
[96] *Id.*, at art. 25.1.
[97] Jorg Rehder & Erika C. Collins, *The Legal Transfer of Employment-Related Data to Outside the European Union: Is It Even Still Possible,* 39:1 Int'l Law. 131 (2005).
[98] Issuance of Principles and Transmissions to European Commission: Procedures and Start Date for Safe Harbor List, 65 Fed. Reg. 45,666 (Sept. 19, 2000).
[99] *Id*. at 45,667.
[100] Pavan Duggal, *Wake-up Call for Indian Outsourcing Industry*, India Abroad, July 8, 2005, at A20.
[101] John Ribeiro, *Indian Law May Satisfy Data Protection Concerns,* Computerworld, April 21, 2004 *available at* http://www.computerworld.com/printthis//2004/0,4814,92557,00.html.
[102] EPIC/PI - Privacy & Human Rights 2000, http://www.privacyinternational.org/s urvey/phr2000/countrieshp.html (last visited Mar. 12, 2006) [hereinafter Privacy & Human Rights 2000].

[103] *Id.*
[104] Information Technology Act, 2000, The Gazette of India, Registered No. DL-33004/2000, *available at* mit.gov.in/it-bill.asp.[hereinafter IT Act, 2000]
[105] IT Act, 2000.
[106] IT Act, 2000,§43.
[107] IT Act, 2000,§43(b).
[108] IT Act, 2000,§65.
[109] IT Act, 2000,§66.
[110] IT Act, 2000,§67.
[111] EPIC/PI - Privacy & Human Rights 2000, http:// www.privacyinternational.org/survey/phr2000/countrieshp.html#fnB40 (last visited Mar. 12, 2006)
[112] *See Govt .Looking at 'Holistic' Legislation on Data Protection*, The Hindu Bus. Line, Dec. 29, 2004 *available at* htttp://www/thehindubusinessline.com/2004/12/39/stories/2004122902370100.htm*;* Bhagowati, *supra* note 62.
[113] Srivastava, *supra* note 34.
[114] *India Plans Data Protection Laws*, Rediff.Com., Nov. 3, 2004, http://www.rediff.com/money/2004/nov/03data.htm.
[115] *Id.*
[116] Moumita Bakshi, *Review of Information Technology Act - Panel may Favour widening of Computer Offices Ambit,* Hindu Line Bus. \Internet Edition, April 3, 2005, *available at* http://www.thehindubusinessline.com/2005/04/03/stories/20050400301760100.htm.
[117] *British Tabloid's Sting has BPOs Hurting over Privacy Violation, supra* note 51.
[118] John Ribeiro, *India's Prime Minister Acts to Tighten Cyberlaws*, June 2005, http://www .cio-asia.com/ShowPage.aspx?pagetype+2&articleid=1751&pubid=5&issueid=52.
[119] *Id.*
[120] Sruti Changanti, *Information Technology Act: Danger of Violation of Civil Rights,* The Econ. & Pol. Wkly, Aug. 23, 2003, *available at* http://mail.sarai.net/pipermail/reader-list/2003-August/003022.html.
[121] *Id.*
[122] Francis Watson, A Concise History of India 136 (1987).
[123] *Id.*
[124] *Id.* at 138.
[125] *Id*. at 139.
[126] Language in India, http://www.languageinindia.com/junjul2002/balridgeindianenglish.html (last visited April 3, 2006).
[127] *See* World Fact Book, *available at* http://www.cia.gov/cia/publications/factbook/goes/in.html#Intro (last visited Jan. 10, 2006). For example, residents of Kerala speak Malayalam, while residents of the adjacent state of Tamilnadu speak Tamil, and residents of another adjacent state, Karnataka, speak Kannada.
[128] As noted by Madhu Rao, "…fluency in English is often confused with an understanding of idiomatic expressions. The expression 'score a touchdown' may make as little sense in a country whose national sport is cricket as would 'hitting a sixer' in the United States. In interacting with offshore personnel, managers should be careful to avoid culturally unique references. *See* Madhu Rao, *Key Issues for Global IT Sourcing: Country and Individual Factors*, INFO. SYS. J. 19 (Sum. 2004) *available at* http://www.ism-journal.com.
[129] Geert Hofstede, Culture's Consequences: International Differences in Work-Related Values 25,26 (Sage Publications, 1980).
[130] *Id.*; Geert Hofstede, Cultures and Organizations Software of the Mind: Intercultural Cooperation and its Importance for Survival (McGraw-Hill, 1991); F. Trompenaars, Riding the Waves of Culture: Understanding Diversity in Global Business (Irwin1994).
[131]GEERT HOFSTEDE, CULTURE'S CONSEQUENCES: COMPARING VALUES, BEHAVIORS, INSTITUTIONS, AND ORGANIZATIONS ACROSS NATIONS, 79 (Sage Publications, 2001).
[132] *Id.* at 145.
[133] *Id.* at 209.
[134] *Id.* at 279.
[135] P. Maria Joseph Christie,Ik-Whan G. Kwon, Philipp A. Stoeberl & Raymond Baumhart, *A Cross-Cultural Comparison of Ethical Attitudes of Business Managers: India, Korea and the United States,*46:3 J. of Bus. Ethics 263 (Sept. 2003).
[136]Hofstede, *supra* note 154. The data presented here are based on surveys that Hofstede completed in subsidiaries of IBM in 72 countries in 1968 and, again, in 1972. His research generated a database of more than 116,000 questionnaires with respondents matched by occupation, age, and gender. Additional data were generated by later research and were matched across countries.
[137] *Id.* at 107.
[138] *Id.*
[139] *Id.*
[140] *Id.* at 116.
[141] *Id.* at 170.
[142] *Id.* at160, 161, 169.
[143] *Id.* at 298.
[144] *Id.* at 318.
[145] *Id.* at 236
[146] *Id.* at 212
[147] *Id.* at 227
[148] *Id.* at 244
[149] *Id.* at 251
[150] *Id.*
[151] *Id.* at 360
[152] *Id.* at 367, 369
[153] *Id.* at 366
[154] Sandra J. Milberg, Sandra J. Burke, H. Jeff Smith & Earnest A. Kallman, *Values, Personal Information Privacy, and Regulatory Approaches,* 38:12 Communications of the ACM 67 (Dec.. 1995).
[155] *Id.*
[156] Alan Westin, Privacy and Freedom (1967).
[157] Milberg et al., *supra* note 179.
[158] *Id.* at 72.
[159] *Id.*
[160] Sandra J. Milberg, H. Jeff Smith & Sandra J. Burke, *Information Privacy: Corporate Management and National Regulation,* 11:1 Org. Sci. 39 (Jan-Feb. 2000).
[161] *Id.* at 44.
[162] *Id.* at 47.
[163] Privacy International, *Privacy and Human Rights, available at* http://www.gilc.org/privacy/survey/intro.html [hereinafter Privacy International] (last visited Apr. 28, 2005). *See* Barbara Crutchfield George, Patricia Lynch & Susan J. Marsnik, *U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive,* 38:4Am. Bus. L. J. 735, 744 (2001).
[164] Barbara Crutchfield George, Patricia Lynch & Susan J. Marsnik, *U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive,* 38:4Am. Bus. L. J. 735, 744 (2001).
[165] OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data, O.E.C.D. Doc. 58 final, Sept. 23, 1980 *available at* http://wwhttp://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html (last visited July 24, 2005) [hereinafter OECD Privacy Guidelines].Established in 1961, the OECD is an intergovernmental organization of twenty-nine member nations that provides a forum to study and formulate economic policies and to promote mutual trade cooperation. *See* Peter P. Swire & Robert E. Litan, None of Your Business 24 (1998).
[166]OECD Privacy Guidelines *available at*

http://wwhttp://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html (last visited July 24, 2005).
[167] Privacy International, *Privacy and Human Rights, available at* http://www.gilc.org/privacy/survey/intro.html [hereinafter Privacy International] (last visited Apr. 28, 2005).
[168] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Eur. T. S. no. 108 [hereinafter Council of Europe Convention].
[169] *Id.,* art.4, 1; OECD Privacy Guidelines, *supra* note 191, ¶ 19.
[170] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Eur. T. S. no. 108, art. 12, 2; OECD Privacy Guidelines, *supra* note 182, ¶.16 & 17.
[171] Council of Europe Convention, *supra* .note 184, art. 13, 3, b; OECD Privacy Guidelines, *supra* note 191, ¶ 17.
[172] IS/IEC 17799:2005. Information Technology standards are produced jointly by the International Standardization Organization (ISO) and the International Electrotechnical Commission and published by the ISO/IEC Informational Technology Task Force. There is also BS 7799-1 and BS 7799-2 which were first published by the British Standard Institute (BSI) in 1995. BS 7799-1 was later withdrawn and replaced by ISO/IEC 17799. BS 7799-2 still exists and the current version is BS 7799-2:2002. BS7799-2 is being fast tracked by ISO and will ultimately become 27001, perhaps at some point in the future becoming part of an ISO 27000 series of standards.
[174] ISO § 12.1.5.
[175] ISO 17799 §8.1.3.
[176].ISO 17799 §6.3.1.
[177] P. Amy Monahan, *Note: Deconstructing Information Walls: the Impact of the European Data Directive on U.S. Businesses*, 29 Law. & Pol'y Int'l Bus. 275, 283 (1998).
[178] Peter Blume, *The Citizen's Data Protection*, 1 J. Info. Law. and Technology (1998).
[179] *See* Joel R. Reidenburg, *The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services*, 60 Fordham L. Rev. 137,142 (1992); Monahan, *supra* note 202, at 275, 283.
[180] George, Lynch & Marsnik, *supra* note 189, at 743.
[181] Graham Pearce and Nicholas Platten, *Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective*, 22 Fordham Int'l L.J. 2024, 2026 (1999).
[182] Angela R. Broughton, Donald C. Dowling, Jr., David Larson, Holly M. Robbins, & James M. Zimmerman, *International Employment*, 33 Int'l Law. 291, 292 (1999).
[183] FCRA, 15 U.S.C. § 1681.
[184] GLBA, 15 U.S.C. §§6801 *et seq.,* Pub. L. No. 106-202, 113 Stat. 1338.
[185] HIPAA, Pub. L. No. 104-191.
[186] SOX, Pub. L. No. 107-204, 116 Stat. 745, codified at 15 U.S.C. § 7201
[187] George, Lynch & Marsnik, *supra* note 189, at 746.
[188] Patrick.J. Murray, *The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet this Standard?* 21 Fordham L. Rev. 932, 971 (1998).
[189] Privacy & Human Rights 2000, *supra* note 127.
[190] Sudha Nagaraj, *BPOs Will Soon Have Some Privacy,*Fin. Times Info. Service, July 28, 2004, LEXIS. *See Data Protection Post-Haste,* Fin. Times Info. Service, Jan. 3, 2005, LEXIS
[191] Indrajit Basu, *Bureaucratic Corruption Worries India,* United Press Int'l, , Oct. 9, 2003, LEXIS.
[192] Das, *supra* note 19, at 25, 26.
[193] *Id.* at 94.
[194] *Id* at 92.
[195] *See* The British Raj inIndia, S. M. Burke & Salim Al-Din Qraishi (Oxford Univ. Press 2004). British Raj was the name given by the Indians to their colonial rulers, using the Hindi word "Raj", which means "sovereignty," as a derivative of the name used to refer to its own former rulers, the maharajas.
[196] Basu, *supra* note 216.
[197] Examples of the frustrations of the overregulated business environment include the situation encountered by the Tata family, well respected entrepreneurs in India who owned Air India before it was nationalized. The Tatas allegedly made 119 proposals between 1960 and 1989 to start new businesses or expand old ones and all of them were rejected by the government workers. Das, *supra* note 19, at 93.
[198] *Id* at 202.
[199] *Id*. at 97. "License-Permit Raj" is "a phrase used to describe the system of allotting industrial and commercial permits to expand or initiate production ventures under government regulations." As referred to above, the word Raj means "rule" or "sovereignty" and "has historically been used to refer to British rule, hence the pejorative usage." *See License-Permit Raj,* Asia Reference, http://www.asiasource.org/reference/display.c fm?wordid=1848 (last visited Aug. 11, 2005).
[200] Monopolies and Restrictive Trade Practices, Act, Act No.54 of 1969. The Monopolies and Restrictive Trade Practices Act included a provision that declared that "any group with combined assets above U.S.26.7 million was a monopoly and effectively debarred from expanding its business after 1969." Das, *supra* note 19 at 168, 169.
[201] Foreign Exchange and Regulation Act, Act No. 46 of 1973. One of the reasons this law was passed was to regulate the import and export of currency for the conservation of the foreign exchange resources of the India "and the proper utilization thereof in the interest of the economic development of the country."
[202] Barbara D. Metcalf & Thomas R. Metcalf, A Concise History of India, at 255, 256 (California University Press, 2002). Many of the telecommunication improvements can be attributed to Sam Pirtroda who headed the Telecom Commission and was chief technical advisor under Prime Minister Rajiv Gandhi. He interceded at the time of Jack Welch's visit to India in 1989 to break through the red tape so that General Electric could begin using India as an outsourcing venue. *See* Das, *supra* note 19, at 207-210.
[203] Solomon *supra* note 16.
[204] Das, *supra* note 19, at 216.
[205] Directive, *supra* note 10.
[206] Nanda, *supra* note 7.
[207] *See* Offshore Outsourcing of Data Services by Insured Institutions, *supra* note 5.
[208] *Id.*
[209] *Id.*
[210] Cal. Civ. Code §1798.82 (West 2003).
[211] *Outsourcing and Offshoring: Unpatriotic or Not - Legal Considerations Are a Must*, Mondaq Business Briefing (July 16, 2004), LEXIS.
[212] *Data Privacy on Government Radar, Finally,* Fin. Times Info, Mar. 21, 2004, LEXIS
[213] The ISO1799 Community Portal, http://www.1799.com. (last visited June 28, 2005).
[214] British Standard 7799 (ISO 17799*),* http://www.knowledgeleader.com/iafreewebsite.nsf/content/SecurityBritishStandard7799ISO17799?OpenDocument (last visited June 28, 2005).
[215] There are a number of third party organizations that qualify as accredited certification bodies that assess the management system against the standard BS 7799-2/ISO 17799.
[216] Arbitration institutions that can be used to administer the arbitration program include the Paris-based International Chamber of Commerce Court of Arbitration and the international division of the American Arbitration Association - the International Center for Dispute Resolution. *See* James W. Morando & Nan E. Joesten, *Leverage Points in International Arbitration,*11:3 IP Litigator, May/June 2005, LEXIS.
[217] The 1996 Arbitration and Conciliation Act provides for the enforcement of awards covered by the 1923 Geneva Protocol, the 1927 Geneva Convention and the 1958 United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards, i.e., the New York Convention to which India is a party. *See* Ravi Nath, (Legal *Issues in Offshore Outsourcing), Enforcement of Foreign Awards in India*, presented by Molly Doland, Shaw Pittman LLP, the Amercan Bar Association Convention, Section of International Law and Practice, Aug., 2004, Atlanta, GA..
[218] *See* Hofstede, *supra* note 156, at 235.
[219] *See* Srivastava, *supra* note 34. It has been reported that India's export in the BPO sector in 2004-05 has reached U.S.$5.2 billion and the projection for the coming year is U.S.$7 billion.

[220] *See Philippines, Eastern Europe Challenge India's Supremacy,* New India Times, March 7, 2005.
[221] *See* Pratap Ravindran, *Factors that are Worrisome for BPO Sector,* Fin. Times Info., April 3, 2004.
[222] Fair Credit Reporting Act, 15 U.S.C. § 1681 (2003).[hereinafter FCRA].
[223] *Id.,* 15 U.S.C. § 1681 (g)(a)(1).
[224] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (1996). [hereinafter HIPAA].
[225] Financial Services Modernization Act, 15 U.S.C. §§6801 *et seq.,* Pub. Law No. 106-202, 113 Stat. 1338 (1999). [hereinafter GLBA]. *See* Testimony of Amy S. Friend, Assistant Chief Counsel of the Office of the Comptroller of the Currency, Committee on Senate Banking, Housing, and Urban Affairs, March 10, 2005, LEXIS.
[226] *Id.*
[227] Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745, codified at 15 U.S.C. § 7201 (2002). [hereinafter Sarbanes-Oxley or SOX].
[228] Mark E. Harrington, *Safeguarding Corporate Information,* Calif Bar J., March 2005, at 10.
[229] SOX, § 404(a).
[230] HHS Fact Sheet, *Protecting the Privacy of Patients' Health Information: Summary of the Final Regulation*, Dec. 20, 2000, *available at* http://www.hhs.gov/news/press/2000pres/00fsprivac y.html .
[231] 45 CFR Part 164.308(a)(6) (Oct. 1, 2005)
[232] Title 45 C.F.R. Parts 160, 164. *See* Michael L. Ziegler and Alan H. Sonnenklar, *Beneficial but Tricky; Numerous, Complex Regulatory Issues Must Be Identified and Addressed,* N. Y. Law J., Aug. 30, 2004, LEXIS.
[233] The Gramm-Leach-Bliley Act. The Financial Privacy Rule, *available at* http://www.itc.gov/privacy/privacyinitiative/finacialrule/html (last visited April 2, 2006).
[234] The GLBA defines "Nonpublic personal information" as any information that a financial institution collects about an individual in connection with providing a financial product or service to an individual, unless that information is otherwise publicly available. This includes basic identifying information about individuals, such as name, Social Security number, address, telephone number, mother's maiden name, and prior addresses. *See* 65 Fed. Reg. 33,646, 33,680 (May 24, 2000) (the FTC's Privacy Rule).
[235] Privacy of Consumer Financial Information, 16 C.F.R. Part 313 (Jan. 1, 2006). (GLBA Privacy Rule).
[236] Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and soundness, 66 Fed. Reg. 8,616-14 (Feb. 1. 2001). *See* Prepared Statement of the Federal Trade Commission before the Committee on Banking, Housing, and Urban affairs, U.S. Senate on Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information, March 10, 2005, *available at* htttp://www.ftc.gov/opa/2005/03/idhefttest.htm.
[237] Harrington, *supra* note 107.
[238] 15 U.S.C. §§6801 *et seq.,* Pub. Law No. 106-202, 113 Stat. 1338. *See id.*
[239] Cal. Civ. Code §1798.81.5 (b) (West 2006). *See* Harrington, *supra* note 107.
[240] Cal. Civ. Code §1798.81.5 (c) (West 2006). *See* Harrington, *supra* note 107.
[241] Cal. Civ. Code §1798.81.5 (d)(1) (West 2006). *See* Harrington, *supra* note 107.
[242] Cal. Civ. Code §1798.82 (West 2006). *See* Harrington, *supra* note 107.
[243] Cal. Civ. Code §1798.82 (West 2006).
[244] *Id.*
[245] *Id.*