Data Protection in India: The Legislation of Self-Regulation

Adrienne D’Luna Directo*

Abstract: As the importance of data privacy has garnered national and global attention over the past two decades, nations around the world have struggled to effectively and timely regulate the protection of sensitive personal information. India, the widely recognized country of choice for outsourcing, faces stiff competition from countries seeking to capture some of India’s outsourcing market share. The Indian Central Government and Indian outsourcing firms thus have a particular stake in assuring American and European corporations that their data privacy concerns are being proactively addressed. This Comment explores the history of outsourcing, including the popularity of outsourcing as a corporate cost-savings mechanism, and why India has been favored by corporations in developed nations seeking viable outsourcing destinations. Additionally, this Comment discusses data privacy and its relation to outsourcing, and concludes that the Indian Central Government has a unique opportunity to leverage the work done by the Data Security Council of India—the Indian Information Technology-Business Process Outsourcing industry’s self-regulatory organization—to ensure that Indian outsourcing firms adhere to a more comprehensive regulatory regime governing data privacy. By utilizing its opportunity, India can maintain its position as the outsourcing destination of choice for American and European corporations.

* J.D., 2014, Northwestern University School of Law; B.A., 2007, English, University of California, Berkeley. I thank the editors of the Northwestern Journal of International Law & Business for their hard work and generous insights, as well as Alfonso Directo, Debra D’Luna, and Lionel D’Luna for their consistent support and encouragement.
# TABLE OF CONTENTS

I. Introduction .......................................................................................... 3

II. Outsourcing: A Primer .......................................................................... 4
    A. Why Companies Outsource ......................................................... 5
    B. Outsourcing to India .................................................................... 6

    A. Historical Evolution of Data Privacy on an International Scale ... 9
    B. Models of Privacy Protection and Adoption by Nations .......... 10
    C. Existing Data Privacy Laws ......................................................... 12
    D. Who Are We Protecting? .............................................................. 18
    E. What Happens When Data Privacy is Not Protected? .......... 18

IV. Analysis .................................................................................................. 20
    A. Today, Companies Look for More When They Outsource .... 20
    B. Surviving the EU Directive ......................................................... 24
    C. Finding Continued Success with American Companies ....... 25

V. Recommendations .................................................................................. 26
    A. The Legislation of Self-Regulation: Adopt an SRO .......... 26
    B. Enforcement Through DSCI Membership ......................... 27

VI. Conclusion ............................................................................................ 30
I. INTRODUCTION

As the importance of data privacy has garnered national and global attention over the past two decades, 1 nations around the world have struggled to determine how to best regulate the protection of sensitive personal information. Many of the nations choosing to regulate data privacy are developed countries whose commercial sectors have an interest in minimizing risk from unprotected data. 2 This Comment argues that just as the United States, the European Union, and other developed nations have an interest in guarding data privacy, India, the widely recognized country of choice for outsourcing, 3 must also develop an interest in and mechanism for protecting data. India has benefitted tremendously from commercial outsourcing. In fact, in 2011, 26% of surveyed Chief Financial Officers favored India for their company’s outsourcing needs. 4 However, because international competition for outsourced services has increased, American and European companies may seek new destinations that better meet their needs 5 unless the Indian outsourcing industry can cultivate and maintain a reputation for providing unique value, including data protection. 6 India and Indian outsourcing firms thus have a particular stake in assuring American and European corporations that their data privacy concerns are being proactively addressed.

Part II of this Comment provides a history of outsourcing and explains why outsourcing is a popular corporate cost-savings mechanism. The discussion then describes India’s historical role as the original destination for overseas outsourcing and its present status as the world’s leading provider of outsourcing services. Part III addresses the issue of data privacy, including various interpretations of the term and several global approaches to regulating data, in order to provide context for the present importance of data privacy protection and its relation to outsourcing.

---

6 For example, the number of voice contracts that have moved from India to the Philippines in recent years illustrates the competing Filipino value proposition of culture quotient. In order to retain Business Process Outsourcing contracts, Indian outsourcing firms must respond by offering something different: enhanced technology capabilities including data protection. Goutam Das & Sunny Sen, Born Again, BUSINESS TODAY (Apr. 1, 2012), http://businesstoday.india/ni/story/bpo-future-india/1/22946.html; see also Preetam Kaushik, Indian BPO: Bright Past, Cloudy Future, BPO OUTCOMES (July 11, 2012), http://bpooutcomes.com/indian-bpo-past-future/.
Finally, Part IV analyzes the Indian Information Technology-Business Process Outsourcing (IT-BPO) industry and a discussion of the guidelines promulgated by its self-regulatory organization, the Data Security Council of India (DSCI). Part V provides recommendations for how the Indian Central Government can leverage the work done by the DSCI in amending its Information Technology Act to provide for more comprehensive data privacy regulation and enforcement over information technology.

II. OUTSOURCING: A PRIMER

In the 1990s, outsourcing referred to contracting with a third-party vendor for a specific service rather than sending work abroad, and the notion of hiring a foreign company to perform a specific business function was known as offshoring. In recent years, however, outsourcing has become synonymous with sending jobs and operations abroad, and the distinction between outsourcing and offshoring has all but disappeared. Thus, outsourcing can be defined as “the practice of transferring the entire responsibility for business process or information technology applications development to an external service provider – often overseas – to reduce costs and achieve a competitive advantage.”

Outsourcing has become popular for a range of services, and the industry is categorized by more specific labels: Information Technology Outsourcing (IT Outsourcing), Business Process Outsourcing (BPO), Finance and Accounting Outsourcing, Knowledge Process Outsourcing, Human Resources Outsourcing, Legal Process Outsourcing, Document Process Outsourcing, and Educational Services Outsourcing. IT-BPO is frequently treated as a single outsourcing category because IT Outsourcing and BPO share many common features including operational cost savings. This Comment focuses on IT-BPO because it is a rapidly growing outsourcing sector utilized by a wide breadth of industries. IT-BPO includes support for maintaining computer hardware and software systems, support operations, telecommunications, call centers, document processing, payroll and human resources management, insurance claims, accounting services, financial service processing and operations, market research, and

---

8 Id.
10 Globalex Solutions, Outsourcing: One Tree, Many Branches, JD SUPRA (Sept. 29, 2010), http://www.jdsupra.com/legalnews/outsourcing-one-tree-many-branches-26273/.
A. Why Companies Outsource

While companies cite many reasons for outsourcing, the opportunity to reduce operational costs is a primary driver. The comparatively low cost of labor available overseas makes it possible for a company to hire multiple workers abroad for the price of just one domestic worker. Also, IT-BPO generally has low startup costs because the functions being outsourced do not require expensive infrastructure.

12 Sorey, supra note 7; Yuen, supra note 9.
15 Disclosure of confidential data is a primary concern, and companies that rely on BPO providers’ confidentiality, such as American insurer Travelers Indemnity Company, are quick to terminate provider relationships when a breach occurs. See Chandra R. Srikanth, EXL Loses Key Client Due to Breach of Confidential Data, ECON. TIMES (Nov. 6, 2013, 4:11 AM), http://articles.economictimes.indiatimes.com/2013-11-06/news/43733313_1_termination-notice-client-bpo. Also, perpetrated cybercrime suggests that BPO providers may be targeted as weak links in data security like in May 2013 when Pune-based payments processor ElectraCard Services suffered a security breach as part of a $45 million ATM heist of two Middle Eastern banks. See Joelle Mendonca, IT Services Companies Under Attack from Cyber Crooks, ECON. TIMES (May 14, 2013, 6:50 AM), http://articles.economictimes.indiatimes.com/2013-05-14/news/39256330_1_data-breach-data-security-council-kamlesh-bajaj; see also Dinesh Nair & Jessica Dye, Indian Card Processor in $45 Million Heist is ElectraCard: Sources, REUTERS INDIA (May 11, 2013, 6:13 PM), http://in.reuters.com/article/20130511india-crime-cybercrime-india-idINDEE94A04620130511. There is even some evidence that companies relying on BPO may actually leverage their BPO as a means for hiding company-perpetrated abuses. For example, in September 2012 Standard Chartered Bank agreed to pay New York’s Department of Financial Services a $340 million civil penalty to settle allegations that it hid transactions with Iran from regulators by using the services of its BPO subsidiary in Chennai to cover up its scheme. The facts of the Standard Chartered case suggest that the BPO subsidiary may have been merely a pawn in the bank’s scheme to launder money. See Standard Chartered Inks $340 Million Deal with NY Regulator, REUTERS (Sept. 21, 2012, 2:55 PM), http://www.reuters.com/article/2012/09/21/us-standardchartered-settlement-idUSBRE88K10420120921; see also Jessica Silver-Greenberg, British Bank in $340 Million Settlement for Laundering, N.Y. TIMES (Aug. 14, 2012), http://www.nytimes.com/2012/08/15/business/standard-chartered-settles-with-new-york-for-340-million.html?pagewanted=all.
18 Sorey, supra note 7.
19 Yuen, supra note 9, at 49.
Low-cost labor can allow speedy realization of significant cost savings, but this is just one of many costs to be considered when a company decides whether to outsource its operations.\(^2\) For example, the determination of whether to engage IT-BPO services also involves consideration of the expenses associated with searching for an IT-BPO provider, contract negotiation, governance, risk-mitigation measures that a company may need to adopt,\(^3\) and finally, any potential customer backlash that could result from the decision to outsource jobs or from a potential data privacy breach.\(^4\)

B. Outsourcing to India

The offshore outsourcing industry began in India, and today India retains its position as the global destination for offshore outsourcing.\(^5\) Companies cite many economic, political, and cultural incentives for choosing to outsource to India, including its probusiness, entrepreneurial climate, and historical ties to the United States and United Kingdom.\(^6\) Additionally, India’s low-cost, high-quality workforce includes many English speakers with advanced educational credentials.\(^7\) India’s stable

\(^2\) See id.
\(^3\) Id.
\(^4\) In a 2006 survey by global advisory and consulting firms Capgemini and IDC of almost 300 executives regarding BPO best practices, 23.5% of survey participants considered public and customer backlash to be the biggest downside to outsourcing. Companies Look for Outsourcing Providers to Drive Innovation as Well as Reduce Costs According to Capgemini/IDC Annual Survey: More Than Half Surveyed Believe Outsourcing Has Met or Exceeded Their Expectations – Almost a Third Say Too Early to Tell, BUS. WIRE (Mar. 30, 2006, 9:00 AM), http://www.businesswire.com/news/home/20060330005154/en/Companies- Outsourcing- Providers- Drive- Innovation- Reduce- Costs [hereinafter Companies Look for Outsourcing Providers].

India, CLUTCH, http://www.sourcingline.com/outsourcing-location/india (last visited Mar. 12, 2014).\(^8\)


\(^6\) While India suffers a literacy problem that suggests a comparatively small educated workforce, India currently has a population of approximately 1.27 billion people, 12% of whom obtain higher education at one of India’s more than 600 universities and 33,000 affiliated colleges. Thus, there is still a vast excess of qualified workers in comparison to the availability of jobs in India. See India Population 2013, WORLD POPULATION STATISTICS (Sept. 19, 2013), available at http://www.worldpopulationstatistics.com/india-population-2013; see also Ranjit Goswami, Economic Growth and Higher Education in India and China, E. ASIA FORUM (July 13, 2012), http://www.eastasiaforum.org/2012/07/13/economic-growth-and-higher-education-in-india-and-china/; Yojana Sharma, India: The Next University Superpower?, BBC NEWS (Mar. 2, 2011, 9:32 PM), http://www.bbc.co.uk/news/business-12597815. Additionally, in 2009 India adopted an ambitious National Skills Development Program to address the need for growth of its educated population.

democratic government, ready adoption of information technology, and convenient geography—which facilitates around-the-clock work—make India an obvious locale for companies considering outsourcing.

In addition to these generally attractive characteristics, other features may make India a particularly strong fit for industries looking to outsource operations. For example, the Legal Process Outsourcing industry is overwhelmingly concentrated in India because the country’s common law underpinnings and similar legal educational system provide much of the underlying foundation required for nuanced legal processing.

Within the past decade, outsourcing has been a dependable source of growth for the Indian economy. For example, in 2012 outsourcing companies created more than two million jobs and comprised 6.4% of India’s Gross Domestic Product, according to India’s National Association of Software and Services Companies. Moreover, the Indian government estimates that its national outsourcing market is worth approximately $52 billion. BPO and Knowledge Processing Outsourcing are the two major outsourcing industries in India, with banking and financial services comprising nearly 40% of the outsourcing services delivered.

While outsourcing has increasingly become a critical component of the Indian economy, competition for outsourcing dollars is stiff according to the outsourcing research organization Clutch, with over thirty-five countries receiving an Overall Outsourcing Index of over 4 out of 10. While India tops the list with an Overall Outsourcing Index rating of 7.1, Indonesia, Estonia, and Singapore are not far behind with ratings of 6.7, 6.6, and 6.5 respectively. Indonesia, Bulgaria, the Philippines, and Egypt all surpass India’s Cost Competitiveness rating of 8.3 with respective ratings ranging from 8.6 to 9. These ratings suggest that companies that value cost over

---

27 For example, India’s capital New Delhi operates on a 9.5- or 10.5-hour time difference from the United States’ Eastern Time Zone (the seasonal variation hinges on whether the United States is on Daylight Savings Time). See The World Clock - Time Zone Difference from India — Delhi — New Delhi, TIME & DATE, http://www.timeanddate.com/worldclock/difference.html?p1=176 (last visited Jan. 26, 2014).
28 See Krishnan, supra note 24, at 2207–11.
32 Outsourcing Industry, supra note 30.
33 Clutch compiles outsourcing statistics by country and provides rankings on a scale of 1 to 10, with 10 being the highest score, across dozens of key statistics which fall into three broad areas: Cost Competitiveness, Resources and Skills, and Business and Economic Environment. Top Outsourcing Countries, supra note 3.
34 Id.
35 Id.
other factors may not view India as the best choice for IT-BPO services. Because over 90% of India’s business in IT and BPO outsourcing comes from the Americas and Europe, India has a vested interest in continuing to provide effective and low-cost solutions for American and European outsourcing needs.

Additionally, while the 2008 recession provided a fertile environment for the growth of IT-BPO outsourcing, speculation abounds that growth will slow due to a convergence of influences, including technological advances, economic uncertainty, pressure to bring jobs back in-house, and a growing desire by companies for internal control over operations. Backsourcing, or “the taking back in house of previously outsourced services,” has more recently entered the business lexicon as the decisions of select prominent companies suggest this backsourcing trend may be accelerating. Thus, Indian IT-BPO providers may be competing for less potential overall revenue from American and European countries, making it all the more critical that India positions itself as the optimal destination for companies deciding where to send their IT-BPO dollars.

III. DATA PRIVACY: WHAT IS IT, AND WHY DOES IT MATTER?

In the age of the Internet, limitless global transmission of data of all kinds is the status quo. While there are a number of possible interpretations of data privacy, the phrase usually refers to the privacy of information associated with an individual (personal data) or to the privacy of the contents of electronically transmitted communications. This Comment focuses on data privacy as the privacy of personal data or information

36 India, supra note 23.
40 For example, in mid-2012, General Motors announced a three- to five-year strategy to increase the in-house presence of its IT services—a marked change from its prior strategy which relied on 90% of its IT services being outsourced. GM Reverses Gears on Outsourcing, Plans Big IT Overhaul, REUTERS (July 12, 2012, 4:19 PM), http://www.reuters.com/article/2012/07/12/us-gm-outsourcing-idUSBRE86B1BT20120712.
associated with an individual. The notion that this kind of data deserves protection is rooted in the doctrine of an individual’s right to privacy.42

A. Historical Evolution of Data Privacy on an International Scale

Today, the European Union (EU) and the United States consider privacy a fundamental right.43 Within that notion, however, the EU and United States view the concept of personal data very differently.44 In the EU, personal data is considered an individual’s property and is treated as intellectual property.45 This view of personal data is so pervasive that many European countries protect personal data privacy rights in their constitutions.46 Perhaps the EU places a premium on ownership and protection of personal data because of its historical experience with egregious and authoritarian violations of personal privacy by member nations.47 Additionally, EU nations subscribe to a shared philosophy that the most reliable way to protect data is to empower an independent legal body48 to scrutinize existing processes and dole out repercussions for violations as necessary.49

In contrast, the U.S. notion of data privacy evolved from a very different starting point in the late nineteenth century: the common law tort concept of invasion of privacy.50 The U.S. notion of privacy does not focus
on personal data, but rather “the kinds of privacy that have been deemed a fundamental right tend to be related to autonomy,” which is often construed to refer to certain aspects of sexual life or reproduction. Thus, the right to privacy in the United States places limitations on government intrusion into the private lives of U.S. citizens but does not explicitly provide for a right to personal data privacy. For these reasons, U.S. laws regulating transmission of personal data are sparse by European standards, and where they do exist, they do not treat an individual’s access to the individual’s own data as a fundamental right. The U.S. private sector remains largely ungoverned, leaving industries to self-regulate the treatment of personal data in the absence of legislation on the subject.

B. Models of Privacy Protection and Adoption by Nations

As global awareness of the importance of protecting personal data has increased, three primary approaches to data-protection regulation have evolved. Each regulatory approach appears to be rooted in a historical viewpoint on privacy in relation to personal data. EU member nations have adopted a system of comprehensive laws, including a broad data protection law that governs the collection, use, and dissemination of personal information by both the public and private sectors. EU member nations typically designate an official or agency to supervise enforcement of the relevant regulation. This approach is favored by the EU perhaps because of its historical distrust of individual actors to self-regulate given the temptation of corruption. Other nations, such as Canada and Australia, adapted the EU’s system of comprehensive laws into a coregulatory model in which each industry develops enforceable standards for privacy protection that are enforced by the industry and are supervised by private agencies.

---

53 George et al., supra note 45, at 746.
56 George et al., supra note 45, at 746–47.
57 See Banisar & Davies, supra note 54, at 13.
58 Id. at 10.
59 See EU Directive, supra note 48, art. 25.
60 Banisar & Davies, supra note 54, at 13.
61 See George et al., supra note 45, at 743.
62 Banisar & Davies, supra note 54, at 13–14.
Other countries, such as the United States and India, regulate data privacy through specific sectoral laws, which govern data protection in a particular industry or technology rather than through a single, broadly applicable regulation. Most nations that have adopted the sectoral law approach do not rely upon oversight agencies to monitor the effectiveness of current data protection methods. The overall effectiveness of such laws is therefore contingent upon a proactive, informed legislature that enacts applicable laws as technology and regulatory needs evolve. When coupled with comprehensive legislation, sectoral laws can provide an effective way of regulating specific additional details with respect to how to treat certain types of information.

The third regulatory approach to data privacy is self-regulation where in the absence of law companies and industries devise the codes of practice to which they agree to adhere. While the Indian government currently does not espouse this approach, the concept of self-regulation has taken root in India. In 2007, India’s National Association of Software and Services Companies (NASSCOM), a not-for-profit trade association formed by Indian IT and BPO industries, developed the self-regulatory organization (SRO) DSCI to monitor and enforce industry data protection standards. While the DSCI takes a comprehensive approach to addressing outsourcing companies’ concerns regarding data protection, its enforcement power is limited by the very nature of self-regulation, which relies on each industry taking a proactive approach to self-monitoring. Because enforcement is typically the province of law rather than industry self-regulation, this approach presents little more than a positive first step towards reformed behavior and practices unless it is formalized by the Indian government.

In the face of inconsistent data privacy regulation, individuals have turned to privacy technologies to attempt to control the way their personal data is used. Individuals often use commercially available technology-based systems to stave off the potential for personal data violations.

---

63 Id. at 14.
64 Id.
67 DSCI’s mission is “[t]o create trustworthiness of Indian companies as global sourcing service providers, and to assure clients worldwide that India is a secure destination for outsourcing where privacy and protection of customer data are enshrined in the global best practices followed by the industry.” Knowledge Management, DSCI, http://www.dsci.in/taxonomypage/284 (last visited Feb. 16, 2014).
68 See Banisar & Davies, supra note 54, at 14.
69 Id.
70 Commercially available tools from companies such as Symantec assist individuals or companies with the protection of personalized data. Symantec focuses on the protection of customer data through products that provide security, backup and recovery, data availability, and data loss prevention by minimizing risks to information, technology, and processes across a multitude of devices, platforms,
Companies may also adopt this proactive stance by installing more sophisticated tools and technologies to address potential breaches in information security.

Companies seeking to benefit from the cost savings that can be realized through outsourcing place a premium on data security even in the absence of data privacy regulations. Monitoring the usage of personal data on a proactive basis helps these companies avoid hefty litigation costs that could result from a lack of data security. Companies with an interest in minimizing data privacy breaches can actively manage risk by including contractual provisions requiring data privacy in all outsourcing agreements. Thus, even if criminal liability does not exist vis-à-vis regulations, judicial recourse is made available through contractual terms.

C. Existing Data Privacy Laws


71 Banisar & Davies, supra note 54, at 14.


73 Generally, companies retain liability for actions of their outsourcing vendors absent a contractual provision to the contrary. For this reason, companies are concerned about confirming their outsourcing vendors’ compliance with relevant privacy policies. ADVISEN, THE LIABILITY OF TECHNOLOGY COMPANIES FOR DATA BREACHES 4 (2010), available at https://www.advisen.com/downloads/Emerging_Cyber_Tech.pdf.

74 George & Gaut, supra note 24.

75 See Lasprogata et al., supra note 41, at 7–8.

members, including the U.S.” which have formed the bases for many pieces of national legislation that address data privacy concerns. The Council of Europe’s 1981 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data is another piece of seminal background legislation because it established privacy as a European-recognized human right. Together, these two regulations set the stage for the adoption of the EU Data Privacy Directive.

In October of 1995, the EU globalized its data privacy concerns by implementing an unprecedented regulation known as the EU Data Privacy Directive (EU Directive). In keeping with the European perspective on individual privacy as a fundamental right, the EU Directive takes a firm stance on the importance of protecting personal data by limiting global negotiations regarding data privacy. Like all directives issued by the EU, the EU Directive acts not as binding law on member nations but rather as a recommendation, or goal, for legislation that should be adopted by each nation. The EU Directive leaves no doubt that the EU views data privacy as a serious concern, and it boldly asserts extraterritorial authority over non-EU nations.

The EU Directive’s unique and aggressive stance on protecting data privacy has global impacts, including intrusion into U.S. business policies. Article 25 of the EU Directive blocks the flow of information from Europe to nations lacking acceptable privacy protections. Together, Article 25 and Article 26 of the EU Directive address the issue of cross-border transfers of personal data to non-EU nations with startling directness—promulgating a concept known as the “Adequacy Principle.” The Adequacy Principle is significant in that it reaches extraterritorially and permits the transfer of data only to outside countries that provide an “adequate level of data protection.” According to the EU Directive, the adequacy of the level of protection provided in such a cross-border transfer of personal data to a third country is evaluated under the following standard:

77 George & Gaut, supra note 24.
78 Id. at 743–44 n.33.
80 Salbu, supra note 43, at 656.
81 See EU Directive, supra note 48.
82 Id. art 1(1).
83 Salbu, supra note 43, at 689.
84 Id.
85 Id. at 692.
86 George et al., supra note 45, at 736.
87 Id. at 783.
88 EU Directive, supra note 48, art. 25.
89 Yuen, supra note 9, at 63.
90 Id.
[The adequacy of the level of protection] shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in questions and the professional rules and security measures which are complied with in that country.91

Notably, the EU Directive contains a general prohibition on transferring personal data to a third country that does not, as a matter of law, provide adequate data privacy protection.92 However, otherwise noncompliant countries may be exempted from this prohibition if adequate safeguards are enacted.93 The United States, because it does not consider data privacy a tangible personal right94 and it fails to meet the EU Directive’s threshold for having sufficient laws protecting data privacy,95 does not initially meet the adequacy standard laid out in Article 25.96

Consequently, because the United States fails to meet the standard described by the EU Directive’s Adequacy Principle, it has sought and obtained an exemption through the development of International Safe Harbor Privacy Principles (Safe Harbor Principles), which the EU Commission adopted in July 2000.97 The Safe Harbor Principles permit U.S. companies to transfer the personal data of EU residents if (1) consumers are appropriately notified98 and given an opportunity to opt out of disclosure of their personal data (or opt in, for particularly sensitive information), (2) the organization collecting the information takes reasonable steps to protect it,99 and (3) sufficient mechanisms for ensuring compliance with the Safe Harbor Principles are established.100 Even under

91 EU Directive, supra note 48, art. 25(2).
92 Id. art. 26(2).
93 Id.
95 EU Directive, supra note 48.
96 Salbu, supra note 43, at 675.
97 Id. at 680.
98 Appropriate notification includes notifying the customer as to the following: (1) the purposes of the information collection; (2) how they may contact the company with questions or complaints; (3) the types of third parties that the information will be disclosed to; and (4) how to limit use and disclosure of their personal data should the company be misrepresenting its use of the information. MICHAEL D. SCOTT, SCOTT ON COMPUTER INFORMATION TECHNOLOGY LAW § 16.32 (3d ed. 2013).
99 Id.
100 Mechanisms for ensuring compliance must include the following: (1) available, independent, and affordable recourse for investigating and resolving an individual’s complaints; (2) follow-up procedures to make sure that participating organizations are using the information in the manner they represented; and (3) a commitment to fix problems resulting from noncompliance with the Safe Harbor Principles and the imposition of consequences. Id.
the Safe Harbor Principles, the EU requires that U.S. companies unambiguously and publicly announce their commitment to comply with the EU Directive’s requirements. For this reason, American companies seeking to be involved in the transmission of EU personal data must certify their adherence to the Safe Harbor Principles by notifying the U.S. Commerce Department of their intent to do so before they may do business with Europe. Additionally, such companies must maintain a privacy policy that conforms to the Safe Harbor Principles at a publicly available location. Other countries have modeled subsequent legislation after the EU Directive, including Canada which enacted a federal Personal Information Protection and Electronic Documents Act in 2001.

The United States has taken an entirely different approach to regulating data privacy, which derives from its common law treatment of the fundamental privacy right as an aspect of autonomy. As mentioned in Part III.B, the United States uses a sectoral approach to regulating data privacy—meaning that industry-based legislation governs the way sensitive personal information must be handled by companies. Thus, the term “breach of privacy” may be inconsistently defined across different industries creating a fractured approach to privacy regulation. This approach is further complicated by the fact that the United States typically regulates data privacy by industry in a reactive manner; it is not until national outcry results from an industry’s failure to protect personal data that the U.S. Congress legislates to remedy the situation. For example, personal health information is governed under a privacy rule called the Health Insurance Portability and Accountability Act (HIPAA), which was enacted as a response to the need for broad healthcare reform. Similarly, in the wake of consumer complaints about the data exposure occurring through financial transactions, the U.S. Congress began to regulate the treatment of personal financial information more closely. Additionally, the landscape of sectoral regulation includes the Financial

---

103 Lasprogata et al., supra note 41.
106 Yuen, supra note 9, at 83–84.
107 See Salbu, supra note 43, at 691.
108 Yuen, supra note 9, at 83.
Services Modernization Act of 1999 (also known as the Gramm–Leach–Bliley Act), which governs personal financial information through Financial Privacy and Safeguards,\footnote{The Financial Privacy Rule and Safeguards Rule are rules promulgated under the Gramm–Leach–Bliley Act. The Financial Privacy Rule mandates that financial institutions must disclose their privacy practices to consumers, while the Safeguards Rule requires that financial institutions protect the consumer data that they collect. Regulation S–P: Privacy of Consumer Financial Information and Safeguarding Personal Information, 73 Fed. Reg. 13692, 13693 (Mar. 13, 2008), available at http://www.sec.gov/rules/proposed/2008/34-57427fr.pdf.} and the Fair Credit Reporting Act, which requires that private sector credit reporting agencies follow strict guidelines for information gathering and provide consumers with access to their information.\footnote{Yuen, supra note 9, at 84.}


The IT Act is India’s most comprehensive data privacy law and covers a significant breadth of subject matter. Sections 4, 5, 7, and 79 of the IT Act contain specific provisions that address data protection for the kinds of information technology frequently involved in outsourcing.\footnote{Id. § 4.} Section 4 protects all electronic information, records, documents, and databases as legal electronic records, which can be proved and produced in a court of law.\footnote{Id. §§ 4, 5, 7, 79.} Section 5 legally recognizes digital signatures as a means of authenticating electronic records and vests the Indian Central Government (Central Government) with the authority to certify companies before they
can legally operate in India and to maintain all digital signature certificates issued under the IT Act.\textsuperscript{121} Under § 7, records must be retained in their originally generated, sent, or received form, and the specific details that identify the origin, date, and time of dispatch or receipt of records must be preserved.\textsuperscript{122} Section 79 exculpates network service providers, including Internet service providers, from liability for the disclosure of third-party data when they can prove that “the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent . . . [against disclosure].”\textsuperscript{123}

In 2006, India demonstrated further awareness of the importance of protecting data privacy, perhaps in response to the EU Directive and negative press around data theft in call centers,\textsuperscript{124} when it passed an amendment to the IT Act that permits the imposition of fines of over $1 million on companies and individuals who fail to adequately safeguard personal information.\textsuperscript{125} While it is important to note that while this is a step in the right direction, this legislation is still problematic for three reasons. First, the legislation is reactionary rather than proactive in responding to the problem of data privacy breaches in the IT industry.\textsuperscript{126} Second, the legislation focuses specifically on the retrieval of personal data instead of the broader protection of personal data and is thus still limited in its regulatory scope.\textsuperscript{127} Third, India has a reputation for lenity in enforcing legislation, which results in a risk to foreign corporations that violations will remain unaddressed.\textsuperscript{128}

As discussed in Part III.B, India also relies on one nonlegal mechanism for promoting data privacy: DSCI, the IT-BPO industry’s self-regulatory organization. The DSCI engages with stakeholders interested in data privacy, thinks proactively about the practical issues around data protection, and strives to address enforcement challenges through innovative solutions.\textsuperscript{129}

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{121} Id. § 5.
\item \textsuperscript{122} Id. § 7.
\item \textsuperscript{123} Id. § 79.
\item \textsuperscript{124} Yuen, supra note 9, at 56.
\item \textsuperscript{125} Id.
\item \textsuperscript{126} Id.
\item \textsuperscript{127} Id.
\item \textsuperscript{128} Id.
\item \textsuperscript{129} According to DSCI’s website, the organization “conducts industry wide surveys and publishes reports, organizes data protection awareness seminars, workshops, projects, interactions and other necessary initiatives for outreach and public advocacy. DSCI is focused on capacity building of Law Enforcement Agencies for combating cyber crimes in the country and towards this, it operates several Cyber labs across India to train police officers, prosecutors and judicial officers in cyber forensics.” \textit{About Us}, DSCI, http://www.dsci.in/about-us (last visited Dec. 2, 2013).
\end{itemize}
\end{footnotesize}
D. Who Are We Protecting?

Implicit in the notion of data privacy regulation, particularly under a sectoral approach, is the idea that a specific population needs protection from impending harm. There are several populations to consider: individual consumers, companies engaged in a business that involves the handling or processing of personal data, and more broadly, local economies. Individual consumers tend to be most concerned about the potential for data privacy violations because they have the most to lose through the unprotected sharing of their personal data, yet they have little ability to ensure adequate data protection measures and they frequently lack effective recourse through which to pursue damages in the case of a breach.

In recent years, companies have become more concerned with whether appropriate data protection measures are being used, both within their organizations and by the outsourcers upon whom they rely. Several multinational companies have been forced to issue public apologies for widespread data breaches. See, e.g., Antone Gonsalves, Global Payments Says 1.5 Million Credit Card Numbers Stolen, CRN (Apr. 2, 2012, 4:23 PM), http://www.crn.com/news/security/232800136/global-payments-says-1-5-million-credit-card-numbers-stolen.htm; Sara Gay Forden, Wyndham Hotels Sued by FTC over Alleged Data Breach, BLOOMBERG (June 26, 2012, 2:39 PM), http://www.bloomberg.com/news/2012-06-26/wyndham-hotels-sued-by-ftc-over-alleged-data-breach.html.

E. What Happens When Data Privacy is Not Protected?

In recent research findings sponsored by PGP Corporation and developed by the Ponemon Institute, analysis from five national cost of data breach studies were consolidated. The countries providing data on recent breaches were the United States, United Kingdom, Germany, France, and Australia.

---


131 Yuen, supra note 9, at 50–51.

132 The Ponemon Institute, founded in 2002, conducts annual consumer studies on privacy trust that are widely quoted by media sources. Why We Are Unique, PONEMON INST., http://www.ponemon.org/about-ponemon.


134 Id.
Figure 1 quantifies the startling costs incurred by each incidence of a data breach. For each country studied, a significant amount of these costs were experienced in the form of lost business as a result of the data breach,\(^\text{136}\) which suggests that consumers pay attention to specific occurrences of data breach—whether personally impacted or not—and adjust their purchasing behaviors accordingly.\(^\text{137}\) Thus, the outsourcing benefits obtained through economies of scale, scope, and specialization are often insignificant in the face of contractual risks that can result from inefficient or incomplete contracts and insufficient oversight of processes.\(^\text{138}\)

Significantly, the results of the aggregated findings also show that the average cost of a data breach to an organization in the United States in 2009 (excluding catastrophic data breach incidents in order to avoid skewing overall findings) was $6,751,451, the highest of the five countries studied.\(^\text{139}\) The average cost of a data breach to an organization across all five countries included in the study was somewhat lower at $3,425,381.\(^\text{140}\) This disparity may be due to the highly varied, sectoral approach to data privacy in the United States in contrast to the more comprehensive data protection laws in Europe. A secondary contributing factor may be that U.S.-based corporations are global leaders in the quantity of digital data

<table>
<thead>
<tr>
<th>Country</th>
<th>Detection &amp; Escalation</th>
<th>Notification</th>
<th>Ex-Post Response</th>
<th>Lost Business</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S.</td>
<td>264,280</td>
<td>500,321</td>
<td>1,514,819</td>
<td>4,472,030</td>
<td>6,751,451</td>
</tr>
<tr>
<td>U.K.</td>
<td>472,883</td>
<td>260,559</td>
<td>662,166</td>
<td>1,170,093</td>
<td>2,565,702</td>
</tr>
<tr>
<td>Germany</td>
<td>1,018,522</td>
<td>181,363</td>
<td>1,058,612</td>
<td>1,186,402</td>
<td>3,444,898</td>
</tr>
<tr>
<td>France</td>
<td>775,047</td>
<td>120,615</td>
<td>866,290</td>
<td>770,170</td>
<td>2,532,122</td>
</tr>
<tr>
<td>Australia</td>
<td>617,015</td>
<td>70,597</td>
<td>529,422</td>
<td>615,697</td>
<td>1,832,732</td>
</tr>
<tr>
<td>Average</td>
<td>629,550</td>
<td>226,691</td>
<td>926,262</td>
<td>1,642,878</td>
<td>3,425,381</td>
</tr>
</tbody>
</table>

\(^{135}\) Id. at 9.
\(^{136}\) Id. at 7.
\(^{137}\) This is confirmed by a 2013 study of over 2,000 U.S. adults commissioned by Cintas Corporation in which two-thirds of those polled responded that they would not return to a business if their personal information was stolen. Press Release, Market Watch, Cintas Study Finds Two Thirds of U.S. Adults Would Not Return to a Business Where Their Personal Information Was Stolen (Oct. 21, 2013, 3:59 PM), http://www.marketwatch.com/story/cintas-study-finds-two-thirds-of-us-adults-would-not-return-to-a-business-where-their-personal-information-was-stolen-2013-10-21?reflink=MW_news_summary.
\(^{138}\) Yuen, supra note 9, at 50.
\(^{139}\) PONEMON INST., supra note 133, at 9.
\(^{140}\) Id.
Data privacy protection matters to companies that outsource because the apparent cost-effectiveness of outsourcing may be undermined by the costs of managing consumer data privacy concerns in the wake of a breach. Because companies that outsource care about data protection, and outsourcing dollars contribute significantly to the Indian economy, data protection should matter to India as well as to other countries that want to secure and retain outsourcing business.

IV. ANALYSIS

The first section below explains why it is critical for companies to consider the quality of current and planned data protection measures when determining whether to begin or continue an outsourcing relationship. It also discusses why India is well positioned to be a continued foreign market leader for IT-BPO and what India must do to maintain this position. The second section below addresses the state of India’s law in terms of supporting the EU Directive’s Adequacy Principle, and suggests why this is relevant to India as a nation and particularly to its IT-BPO outsourcing companies. The last section discusses the likely tasks of U.S. companies that continue to look to Indian outsourcing firms for IT-BPO services particularly in light of the heightened competition within the current economic climate.

A. Today, Companies Look for More When They Outsource

The landscape of data privacy concerns is rapidly evolving. In the past, companies based their outsourcing decisions primarily on the net cost savings that would be realized through outsourcing. When evaluating cost savings, companies focused on the gains that would be realized through near-term cost cutting measures and did not necessarily factor in the costs of a potential data breach. Perhaps companies were focused on

142 Yuen, supra note 9, at 51.
145 Large and prominent data privacy breaches have made companies increasingly aware of their vulnerability to such breaches through inadvertent mishandling of data or, more likely, through cyber attacks. See, e.g., David Kocieniewski, Adobe Announces Security Breach, N.Y. TIMES (Oct. 3, 2013), http://www.nytimes.com/2013/10/04/technology/adobe-announces-security-breach.html?_r=0&wanted=print.

20A
such a narrow definition of cost savings because lawsuits from individual customers on the basis of data privacy breach were unlikely; given the lack of transparency in outsourcing transactions, individuals have difficulty knowing when their data privacy has been breached absent a law requiring disclosure.\footnote{146} Even when individuals become aware that their personal data privacy has been breached, the individuals may discover they have limited legal recourse in addition to limited time and resources to bring a lawsuit.\footnote{147}

Presently, companies still establish outsourcing relationships with the goal of maximizing profit.\footnote{148} However, the critical difference between historical outsourcing goals and today’s outsourcing goals is that now companies recognize that the risk of data privacy breach is a significant component of the cost savings that may or may not be realized through the establishment of an outsourcing relationship.\footnote{149} Thus, companies are more selective in choosing both the geographic location and the outsourcing firm with whom they establish a relationship.

Moreover, companies increasingly acknowledge that some of the biggest challenges surrounding issues of data privacy are the detrimental impacts of a breach upon current and future potential customers. It is not so much a concern about individual lawsuits that may arise as a result of data privacy breaches, but rather the fear of public backlash that might result from a publicized breach that is increasingly motivating corporations to proactively manage their data risk.\footnote{150} Concerns around data privacy and public perception challenges that may result from a breach in personal data are now viewed as avoidable risk.

There is some cause for concern on a macro level that it may be too late to evade the damage that has already been done by past data privacy breaches. American and European companies are increasingly rethinking their business decisions to outsource IT and BPO operations.\footnote{152} There is

\footnote{146} In response to this lack of transparency, privacy rights nonprofit organizations have developed to provide consumers with resources to determine whether their personal data has been involved in a privacy breach. See, e.g., Mission and Goals, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/content/about-privacy-rights-clearinghouse/goals (last visited Mar. 16, 2014).
\footnote{148} Yuen, supra note 9, at 49.
\footnote{149} For example, IBM began walking away from large IT outsourcing contracts when it was unable to negotiate sufficient protection from liability arising from data breaches. Stephanie Overby, IT Service Providers and Customers Battle over Data Breaches, CIO (Mar. 10, 2012, 7:11 AM), http://www.cio.com/article/701890/IT_Service_Providers_and_Customers_Battle_over_Data_Breaches.
\footnote{151} Keynote Address, supra note 150.
growing speculation amongst outsourcing industry analysts that IT and BPO processes will be brought back in-house broadly due to the confluence of these factors: the high-risk reputation of outsourcing, rising labor costs, high outsourcing workforce turnover, and increasing awareness of internal challenges resulting from long-term reliance on outsourcing. Demand for increasing numbers of onshore resources with outsourcing capabilities coupled with recent incidences of fraudulent behavior by outsourcing service providers may contribute to this desire to bring operations back within the internal operations of American and European companies.

There are other reasons that India and its IT-BPO providers should be prepared to face an increasingly competitive outsourcing landscape. After more than a decade of rapid growth, outsourcing is reaching a saturation point in the sense that there are few additional IT-BPO needs left to be outsourced. Outsourcing providers and the economies that benefit from the dollars they bring in must take heed that diminishing growth rate will undoubtedly increase competition amongst individual IT-BPO providers and between countries that specialize in the provision of outsourcing services.

India as a nation is ideally positioned to continue to lead the servicing of outsourcing needs, but in order to maintain its position, India must demonstrate a cognizance of the importance of protecting consumers’ personal data as well as a business-savvy approach to the concerns of American and European countries who currently rely on IT-BPO providers. Recognizing this, Indian outsourcing firms have banded together in recent years to lead data protection reforms that will keep India at the forefront of IT-BPO through self-regulation, and the resulting Privacy Framework and Security Framework suggested by the DSCI are comprehensive and cutting-edge. However, because the DSCI’s enforcement capacity is limited as an SRO, the Central Government must act quickly to demonstrate that regulation of the IT-BPO industry, and the outsourcing industry more

Data Protection in India
35.1A (2014)

broadly, is a national priority. The Central Government has a historical reputation for slowness and lack of enforcement;\(^{159}\) but because NASSCOM and the DSCI have so thoroughly laid the groundwork that would enable direct and effective enforcement, the government only needs to take a few direct steps to legitimize the privacy and security frameworks that many prominent Indian outsourcing firms have adopted.\(^{160}\)

The Central Government has already signaled its awareness of this issue’s significance through legislative gestures\(^{161}\) and the signing of a Memorandum of Understanding with the DSCI indicating the Government’s intent to support its recommended platform.\(^{162}\) Because this is such a critical moment for the future of outsourcing service providers, the time is ripe for the Central Government to move forward with more specific adoption of baseline privacy expectations for its IT-BPO providers. Additionally, because more than 90% of India’s revenue through IT-BPO outsourcing comes from the Americas and Europe\(^{163}\) and India’s economy is heavily dependent on IT-BPO revenue,\(^{164}\) it is especially important that the Central Government look critically at what it can do to proactively position the nation as the geographic and strategic choice for European and American corporations.

As discussed in Part III.B, India’s current approach to data protection is largely sectoral, mirroring that of the United States. However, many American and European companies, concerned by the recent data privacy breaches that have captured international attention,\(^{165}\) are interested in outsourcing to a location where a stricter standard of protection is assured. Rather than expose themselves to risk, these companies would prefer a proactive approach that includes the benefits of outsourcing (such as cost savings and expedited business processes) without the potential downsides of public exposure and liability that could result from breaches of consumer

\(^{159}\) Bali, supra note 13, at 105.


\(^{162}\) See CERT-In Homepage, http://www.cert-in.org.in/ (last visited Dec. 2, 2013). CERT-In is India’s “national nodal agency for responding to computer security incidents as and when they occur.” Id.

\(^{163}\) India, supra note 23.

\(^{164}\) India’s IT-BPO sector provides jobs to approximately 2.8 million professionals, making it one of the largest employment sectors in the nation. Indian IT-BPO Sector Revenue Estimated to Cross USD 100 Billion Mark, NASSCOM, http://www.nasscom.in/indian-itbpo-sector-revenue-estimated-cross-usd-100-billion-mark (last visited Jan. 15, 2014).

\(^{165}\) See, e.g., Overby, supra note 156.
privacy. For this reason, it is critical that India acts quickly to enact privacy legislation focused on the enforcement of data protection. Since Indian outsourcing companies have taken efficient and proactive action to enact industry data privacy measures even in the absence of regulations requiring them to do so, adoption of a legal enforcement mechanism is both timely and necessary to support the portion of the Indian economy that relies on the influx of IT-BPO business from foreign companies.

B. Surviving the EU Directive

In order to survive the heightened standards set in motion by the EU Directive, Indian outsourcing firms have proactively developed measures addressing the provisions of the EU Directive that most directly impact the ways in which European companies now scrutinize their outsourcing providers. Because India was highly successful in attracting European outsourcing business before the EU Directive was implemented, the country stands to lose a great deal if it is unsuccessful in assuring European companies that secure data protection mechanisms have been enacted. Thus, the Adequacy Principle provision of the EU Directive—which again constrains the transfer of personal data to countries with adequate protection measures in place—has significantly impacted Indian outsourcing firms.

The language used in Article 25 that provides for consideration of “the professional rules and security measures which are complied with in that country” when making the determination about whether a third country is adequately protective of personal data has been noted by the DSCI. The Indian outsourcing industry has an immense stake in ensuring that, to the best of its ability, professional rules and security measures are in place to qualify India as a location that may receive cross-border transmission of data from EU member states. In 2006, the Central Government amended the IT Act in reaction to data security concerns in outsourcing firms, but


168 BAJAJ, supra note 65.


170 For a more complete discussion of the Adequacy Principle, see Part III.C.


172 EU Directive, supra note 48, art. 25(2).
Indian outsourcing industry acknowledges this law’s limitation: it fails to establish industry standards for BPO providers or any other category of outsourcer because it focuses on the IT sector. Indian BPO providers have responded to this shortcoming by working collaboratively through DSCI to develop industry standards for the protection of personal data\(^\text{173}\) in the hope that the establishment of self-regulatory mechanisms will provide the requisite adequacy to continue data transmission to Indian outsourcing firms under the EU Directive.

At the time of the EU Directive’s implementation, the Central Government failed to promptly act to create a kind of safe harbor arrangement with the EU, as the United States did. Thus, the Indian IT-BPO industry, through the DSCI, found a way to work around the need to demonstrate adequate protections for personal data under the EU Directive\(^\text{174}\) despite a lack of action by the Central Government. The DSCI has analyzed whether India qualifies to receive cross-border transfers of personal data from the EU under the Adequacy Principle\(^\text{175}\) and has enacted specific self-regulatory guidelines for IT-BPO outsourcing firms to optimize the likelihood that even in the absence of additional national legislation, India will continue to receive outsourcing business from EU member countries.\(^\text{176}\)

C. Finding Continued Success with American Companies

As with the EU Directive, there are some U.S. regulations with which Indian IT-BPO firms must be prepared to comply such as the Gramm-Leach-Bliley Act, HIPAA, and California’s identity protection laws.\(^\text{177}\) However, because of the varied requirements and enforcement mechanisms of these laws, it is unclear how to address data protection in outsourcing relationships. Many American companies monitor their own adherence to these regulations.\(^\text{178}\) In these instances, American companies are looking to find an IT-BPO solution that protects their own immediate interests, but that also offers protection from the regulatory force of these sectoral laws should they be enforced. These companies may therefore consider it doubly important that they work with an outsourcing firm that provides secure mechanisms for protecting personal data as well as recourse in the event of a data breach; these security protocols are what will protect them not only from civil liability to consumers, but also from criminal liability in


\(^{175}\) Id.


\(^{177}\) Yuen, *supra* note 9, at 54.

\(^{178}\) Id.
the event of a data breach.

In the absence of explicit legislation governing the outsourcing services being sought, American companies that are looking to engage in IT-BPO will likely take a slightly different approach from European outsourcers. Because they are less governed by broad standards requiring data privacy protection, these companies are more likely to select specific IT-BPOs that optimally meet their business needs. American companies that seek to engage an IT-BPO provider are also more inclined to understand India’s lack of comprehensive laws protecting data privacy because the United States only regulates specific areas of data privacy by industry. However, for this reason, American companies are more likely to be savvy in the ways in which data privacy can be addressed in the absence of on-point legislation. Understanding this, the DSCI has effectively anticipated how the IT-BPO industry can accommodate the needs of its U.S. clients. The DSCI recommends privacy and security frameworks that incorporate globally recognized best practices to Indian IT-BPO providers as a way of staying ahead of potential U.S. clients’ data privacy concerns.

V. RECOMMENDATIONS

A. The Legislation of Self-Regulation: Adopt an SRO

The DSCI has done a tremendous amount of legwork in analyzing how Indian IT-BPO providers might provide the data privacy protection that EU and U.S. companies seek when considering whether to establish or continue an outsourcing relationship. Additionally, the DSCI has popularized concerns around data privacy apparently to mitigate potential reasons why EU and U.S. companies might choose to scale back their uses of Indian IT-BPO providers in favor of bringing operations in-house or selecting other preferred outsourcing destinations. Thus, while adequately protecting the Indian IT-BPO industry through new data privacy mechanisms might once have proven a formidable near impossibility for the Central Government, private industry has helped to bridge much of the gap by investing its own resources into devising strategies for retaining IT-BPO business in the wake of data privacy concerns. For savvy American corporate consumers of outsourcing services, the assurances provided by

---

180 See, e.g., DATA SEC. COUNCIL OF INDIA, supra note 174.
these self-regulatory measures alone may preserve India’s outsourcing appeal. American companies who themselves are used to looking beyond existing or lacking data protection laws to the true substance of data protection mechanisms in place are likely to be reassured by the extensive protections recommended by the DSCI and adopted by industry members.

B. Enforcement Through DSCI Membership

However, although NASSCOM and the work of the DSCI has brought attention and reform to the Indian IT-BPO industry, the perception that these standards are enforced is still critical to the longevity of the industry, particularly because Indian outsourcing firms are frequently the first targets of criminal allegations when data breaches occur. The Central Government is uniquely well positioned to boost the perception of the IT-BPO industry by adopting reforms that will qualify Indian IT-BPO providers under the EU Directive’s Adequacy Principle, or alternatively, that will provide India with the leverage to negotiate a workaround mirroring the Safe Harbor Principles.

Generally, the Adequacy Principle requires that any third-country transmitter of EU personal data must have a national law regulating data privacy and an agency that enforces that law’s application. Because India has neither comprehensive data privacy legislation nor an active enforcement agency, its IT-BPO providers are navigating a precarious situation despite the self-regulation they have adopted, particularly in light of the increased geographic competition for IT-BPO services as industry growth slows. Although the Central Government is severely deficient in administrative resources, the DSCI’s proactive and comprehensive approach to increasing the data privacy protections used by India’s IT-BPO industry has positioned the Central Government for rapid, low-cost adoption of DSCI recommendations.

The Central Government is thus uniquely poised to leverage the work of the DSCI by amending its most recent and comprehensive data privacy legislation, the IT Act, to include the DSCI as a government agency. While the adoption of more comprehensive legislation regulating data privacy

---

185 George et al., supra note 45, at 763.
186 Banisar & Davies, supra note 54, at 54.
within information technology as well as all industries is desirable, India currently has neither the administrative resources nor the infrastructure to support such broad reform. However, legitimizing the DSCI through governmental adoption in an IT Act amendment would be an achievable first step towards reform that would mutually benefit the interests of the Central Government in maximizing economic growth for India as well as the interests of Indian IT-BPO providers who want to retain European transactions.

Governmental absorption of an SRO is an unusual strategy, but it is one that has been adopted before with some success in another common law nation: the United States. While governmental appropriation of SROs in the United States occurred in the securities industry, a distinctly different arena from data protection, the Central Government could model its approach after the U.S. government’s adoption of securities SROs as an extension of the government. Like the DSCI, American securities SROs began as private sector organizations for industry professionals and organizations. In the United States, SROs were formed to address securities concerns before broad securities laws existed, just like in India where NASSCOM and the DSCI have worked to establish data privacy controls. Similar to the enactment of the U.S. Securities Act of 1933 and the U.S. Securities Exchange Act of 1934—which adopted the most significant SRO measures as federal law—the Central Government could leverage the most significant provisions of the privacy and security frameworks created by the DSCI in a broad amendment to the IT Act.

For a national government like India’s Central Government, there are many advantages to adopting a structure that has already been created by an SRO, including minimal cost to the government in developing legal infrastructure, ease of adoption, and alignment of governmental and industry interests. Because the DSCI has already expended private resources in analyzing the current state of IT-BPO and understanding where privacy protection measures are needed to comply with the Adequacy Principle, the Central Government need not undertake such extensive due diligence in preparation for the enactment of appropriate legislation. Instead, the Central Government can leverage the DSCI’s privacy framework and plentiful analysis to determine the appropriate breadth for an amendment to the IT Act. For ease of enforcement, the Central Government may choose to implement a simplified version of these guidelines just as the U.S. securities laws represent a streamlined form of

190 Id. at 151–52.
191 Id. at 153.
192 Id.
193 Id. at 151.
regulations promulgated by the U.S. securities SROs. Additionally, the Central Government would realize benefits from being aligned with the IT-BPO industry, including the increased national revenue that would result from the international perception of India as a nation that places a premium on the protection of personal data.

Critics of India’s sectoral approach argue that even if India were to enact stricter regulations governing data privacy, without a system-wide reform of the Indian legal process, foreign outsourcers would still have valid concerns about enforcement. However, in addition to laying the groundwork for a well-reasoned amendment to the IT Act, the work done by the DSCI is a critical step towards the implementation of an enforcement mechanism that meets the strict requirements of the Adequacy Principle and quells the fears of foreign outsourcers. The DSCI’s Cyber Labs program has already contemplated the problem of enforcement in detail and has created a multifaceted approach to cybercrime prevention that includes training police, standardizing methods of investigation and promoting cyberforensics. However, beyond making use of the DSCI’s tactical approaches to combating cyber crime, the Central Government has the perfect opportunity to marry enforcement with adherence to DSCI privacy and security principles through an SRO membership structure.

Similar to the U.S. securities industry, where a publicly traded company must comply with SRO rules in order to be listed, the Central Government should adopt a system whereby each Indian IT-BPO provider must obtain and maintain DSCI certification in order to establish itself as a viable option to American and European companies looking to form an outsourcing relationship. Developing a system in which SRO membership is the only way for an IT-BPO provider to be competitive creates an enforcement mechanism that requires minimal expenditure of Central Government resources while maximizing the positive impact on India’s reputation as a nation that prioritizes data protection. Once the IT Act is amended based on the Central Government’s determinations of the DSCI privacy and security frameworks’ most central principles, the Central Government can enlist the help of DSCI, which has already proven itself to be an interested, engaged expert on data privacy, to create membership requirements based on the amended IT Act. The Central Government and the DSCI, working together, must then roll out the enforcement arm of the amended IT Act—an enforceable membership concept in which adherence to DSCI membership requirements is a baseline for participation in India’s IT-BPO industry.

The Indian IT-BPO industry as a whole and the DSCI, as its representative, would also reap large benefits if the Central Government were to adopt an amendment to the IT Act incorporating the most

---

194 Id.
195 See, e.g., Bali, supra note 13, at 125.
significant aspects of DSCI guidelines as law and setting up an enforcement mechanism through DSCI membership. The IT-BPO industry would reap the benefits of having a transparent, regulated industry based on compliance with DSCI principles in the form of continued influx of American and European business. Assuming the amended IT Act plus enforcement through mandatory DSCI membership is sufficient to qualify India as an accepted third-party transmitter under the Adequacy Principle, Indian IT-BPO providers will profit from a steady flow of business from European companies in search of cost effective, EU Directive-compliant outsourcing providers. Even if India does not automatically qualify for approval under the Adequacy Principle, the amended IT Act plus mandatory DSCI membership will help strengthen the IT-BPO industry’s argument that it should qualify for some kind of safe harbor provision. In either case, the adoption of these stricter standards is sure to catch the attention of American companies who are looking to maximize the cost effectiveness of outsourcing by choosing providers who are unlikely to jeopardize customers’ personal data. Thus, Indian IT-BPO providers who comply with DSCI standards stand to gain from the Central Government’s adoption of these measures assuming India can avoid the creation of a black market for services provided by a non-DSCI certified IT-BPO provider.

It is possible that requiring DSCI membership could cause IT-BPO providers to bifurcate into two groups: one that spends money to enact the data privacy protection measures requisite to obtain DSCI membership and another that, to gain a competitive cost advantage, continues with its status quo and as a result can charge American and European companies a much cheaper rate for its services. However, the Central Government can adequately combat such potential detrimental effects by working closely with the DSCI to inform American and European companies of the law and its accompanying membership requirements. Because American and European companies are so hesitant to engage outsourcing providers that do not take privacy protection measures seriously, it is likely that any IT-BPO provider that chooses to ignore the mandatory DSCI membership requirement will simply continue to lose business until it is forced to either become compliant or cease its operations.

VI. CONCLUSION

As electronic transmission of personal data continues to be the bedrock of the outsourcing industry, India, as the global leader in IT-BPO outsourcing, must put a premium on maintaining its national reputation for handling personal data securely. Because public perception suffers every time an organization suffers a large data breach, companies that consider entering into or continuing IT-BPO relationships are highly concerned about minimizing exposure through their outsourcing operations. Additionally, as data privacy continues to garner public attention and
competition amongst outsourcing firms and their nations, companies will be even more likely to take their business to a country that provides them with optimal data security assurances. European companies, under additional pressure to protect consumer data under the EU Directive, will be loath to even consider outsourcing servicers whose countries of origin do not meet the strict standards of the Adequacy Principle.

As a result, the Indian Central Government has particular incentive to leverage the work of DSCI in amending its IT Act to incorporate more comprehensive data protection measures that would strengthen India’s argument that it qualifies under the Adequacy Principle. Because DSCI has developed such a strong baseline framework for privacy protection, the Central Government is optimally positioned to adopt its most significant principles and use DSCI membership as a baseline enforcement mechanism. If the Central Government is successful in adopting these reform measures, India and its IT-BPO industry will realize measurable gains. Additionally, although the global regulatory tide has not yet caught up with technology, legislation like the EU Directive hints that more nations may extraterritorially impose their privacy standards on other nations in the future. For now, India needs to demonstrate that its IT-BPO industry is prepared to operate according to the standards promulgated by the EU so that companies will continue to see it as a prime location for the service of their outsourcing needs.