“Can we trust the Indians with our data?” An examination of the emergence of information privacy laws in India

Ramesh Subramanian
Information Systems Management, School of Business, Quinnipiac University, U.S.A.

Abstract. This paper looks at the nature and current state of evolution of privacy laws in India. India is an emerging economy, but the Indian ITeS environment has already emerged into a mature and highly competitive destination to outsource a variety of business processes from technically advanced nations. There is, however, a tension that exists between the IT industry’s needs and the Indian societal needs in general. One of the causes of such tension pertains to the issue of privacy. An important facet of the IT industry is information privacy – an aspect demanded and expected by its global customers. But the notion of privacy is hardly global. Different countries have different notions of privacy, often based on cultural norms, resulting in widely differing privacy laws. This paper studies the evolution and development of privacy laws from the context of four main players, namely, the law and legal environment, governmental policies, the IT industry and the citizenry of India. The study shows that while India has made several strides in matching the privacy needs of its global clientele, there are several areas which require further work. To some extent, the democratic structure in India, as well as its security needs have made it difficult and cumbersome to enact privacy laws, and more work is required in this area.

1 Introduction

In the last two decades, India has been the beneficiary of the global outsourcing boom. Starting with IT services in the late 1980s the Indian companies providing services to outsourcing companies in the US and UK have steadily grown to encompass other service areas such as business process outsourcing, customer support, research and development in fields ranging from computers science, information technology, manufacturing design and bio-technology, direct marketing, education, health and financial services including tax services and even the entertainment industry such as animation services.

India seems to be a natural destination for global outsourcing. It has a large population of English-speaking technicians, managers, marketers, health professionals and analysts. India's geographic location and the resultant time-differential between itself and technically advanced countries such as the US, Canada and countries of the EU give it an added advantage – when it is night in, say, the US, it is day in India. This gives US companies the possibility of 24-hour shifts which are accomplished by just shifting the work to their Indian counterparts at 5:00pm every day. Global networking as well as other technology developments such as distributed collaborative systems enable seamless transfer of business processes between India and the US, UK and Australia. In addition, even in industries which do not require the daily transfer of job processes between India and US/UK, the availability of Indian workers who are willing to work at nights in order to fulfill the day-time service requirements of US companies, plus the notable wage differential between India and the US provide additional reasons for ensuring the continued boom of outsourcing IT enabled jobs and processes to India in the foreseeable future.

Today, the outsourcing and IT-enabled services industry (ITeS) in India is booming. The Indian IT enabled services sector grew at a rapid rate in the last fifteen years. The earnings from IT-ITES exports was US$ 13.3 billion (61.9 percent of total industry revenues) in 2003-04 and was expected to touch US$ 17.9 billion (63.7 percent) in 2004-05 [1]. Several analysts predict that India will continue to grow in the ITeS arena. According to Noshir Kaka, a partner in McKinsey & Company, "…the total addressable market for global off shoring is approximately $300 billion, of which $110 billion will be offshore by 2010. India has the potential to capture more than 50 per cent of this opportunity and generate export revenues of approximately $60 billion by growing at 25 per cent year-on-year till 2010 [2]."

But this growth is not without its pitfalls. Outsourcing (also known as off-shoring) of business processes has led to job losses in the US and other European countries. This has led to widespread backlash among citizens in these countries, who have been quick to point out some of the problems that have inevitably ensued due to off-shoring. These include communication and collaboration problems exacerbated by distance, differences in work ethics, differences in culture, quality of service issues, and more recently (and ominously), security issues. As the global spread of the Internet increases rapidly, so does the propensity for crime based on exploiting the Internet. These crimes are generally referred to as "cybercrimes," and pertain to criminal activities in which computers and computer networks, notably the Internet, are the tools, targets and locations of criminal activity. As Indian companies grow and become major players in the outsourcing market, Indian professionals working at various locations in India are increasingly involved in directly handling personal data pertaining to citizens of foreign countries, especially from North America and Europe. This raises the issue of data security and safeguarding of privacy of the data.

Certain well-advertised security lapses in Indian ITeS companies have recently come to light which expose the vulnerability of such data to mishandling, theft and other exposure. In April of 2005, three former employees of Mphasis, a BPO company in India, were arrested for defrauding four Citibank account holders in New York to the tune of US$ 300,000. Later, on June 23, 2005, the London-based tabloid, The Sun, reported that one of its reporters was able to buy information about 1,000 UK bank accounts and personal data associated with the accounts from an individual working at an Indian web design company in Gurgaon, a New Delhi suburb [3]. These incidents were widely publicized in the US and UK media, and led to a Forrester Research Report cited in a Rediff.com news article [4] that warned that such incidents will greatly curb the outsourcing boom to India . These incidents, as well as the publicity and the Forrester Reports sent shockwaves to the Indian BPO and outsourcing sectors, which clearly saw the potential for loss of business arising from lax security and protection of data. These developments spurred calls for greater focus on security and privacy in the Indian ITeS sector towards the end of 2005.

The strongest calls to enhance data security and data privacy in Indian ITeS companies have come from the Indian outsourcing industry and NASSCOM (National Association of Software and Service Companies), India. NASSCOM is the main industry association that has historically taken a leadership role in promoting the Indian software industry abroad, in developing standards for the Indian IT industry, in acting as a lobbying group to the government, and in acting as a clearing house for IT industry-related information to domestic and foreign customers.

In this paper we will track some of the governmental, legal and industry-based measures that seek to ensure data security and privacy in India, and, where relevant compare the measures with similar measures that exist in North America and EU countries. The objective of this essay is two-fold. The first is to determine the state of existing instruments to secure privacy in the Indian context. The second is to see if there are significant gaps between the requirements and the reality of the situation in India. Based on these we will finally provide an analysis of privacy in India, and our conclusions and directions for future studies in the area.

In the remaining sections we will discuss the issue of data privacy in India from the points of view of the law, government policies, industry policies and standards, and the people, especially the software industry workers in India.

2. The Indian Constitution's position on an individual's privacy

Privacy is not explicitly guaranteed by the Constitution of India. Article 21 of the Constitution, which was signed in 1949 by Jawaharlal Nehru, the first Prime Minister of India, and went into effect in 1950, states that "no person in the country may be deprived of his life or personal liberty except according to procedure established by law." [5]. This does not explicitly state anything about an individual's right to privacy. The first connection between Article 21's granting of "personal liberty" and an individual's privacy rights in India was established in the 1964

Supreme Court ruling in the Kharak Singh v. State of Uttar Pradesh case [6]. Kharak Singh had complained in his lawsuit that his right to privacy was being violated by the police of the State, who made domiciliary visits to his place of residence and harassed him. In that case, even though the Court repelled Kharak Singh's argument, the minority judgment emphasized the need to recognize the right to privacy "as it was an essential ingredient of personal liberty" [6, para 4]. Since that time, the right to privacy has gradually become accepted as a right granted through Article 21 of the Constitution, and has been applied to various situations including those arising from developments in technology.

In 1994, in the Supreme Court case of R. Rajagopal v. the State of Tamil Nadu, Judge B.P. Jeevan Reddy held that "though the right to privacy is not enumerated as a fundamental right it can certainly be inferred from Article 21 of the Constitution." [6, para 10] Over the years, especially in the mid-twentieth century, even in countries where privacy was considered essential to human existence and personal liberty, the concept of privacy was gradually extended to include matters pertaining to "health, personal communications, family, personal relations and a right to be free from harassment and molestation." [6, para 8].

Despite the gradual recognition of a citizen's right to privacy in India, there is still no general data protection law in India. There are, however, laws that regulate the environment of electronic commerce in India, which is discussed in a later section.

In the following section we will discuss the governmental initiatives and policies pertaining to IT development including data privacy issues.

3. Governmental initiatives in IT and Software development

Even though software outsourcing and on-site software development services were provided by Indian IT firms since the late 1970s, it was the advent of economic liberalization policies in 1984, under Prime Minister Rajiv Gandhi, that gave an impetus to IT development in India. The new policies greatly liberalized the import of computers, peripherals and software to India. Several IT companies generally benefited from this. However, the policies fell short, and did not completely remove many of the import restrictions or the restrictions on travel by Indian software engineers to locations abroad. The foreign exchange shortfall sharply restricted currency exchange between the Indian rupee and the US dollar, which further curbed Indian technocrats from traveling abroad for business purposes. In 1989, India went into an economic recession, and in 1991, Rajiv Gandhi was tragically assassinated, and P.V. Narasimha Rao became the Prime Minister. The country's balance of payment situation became serious in 1991, and India turned to the IMF for assistance. This was followed by a structural adjustment program. The main aim of this program was to increase India's competitiveness through free flow of foreign technology. A New Industrial Policy (NIP) was announced in 1991. Manmohan Singh, the Finance Minister, carried out the economic reforms. Foreign Direct

Investments (FDIs) were permitted in all sectors. Restrictions on software imports were eased further [7].

This led to a tremendous growth in software companies in India. Indeed, India, with its multitude of trained engineers and software professionals, was "at the right place, at the right time," to exploit the emerging need for low cost software and IT enabled services among technically advanced countries. Realizing the vast potential to move India into the echelons of technically advanced countries through using the vehicle of information technology, the Indian government began to take some critical steps towards fostering and engendering growth in this sector. In 1998, Prime Minister Atal Behari Vajpayee set up a "National Task Force on IT and Software Development." The stated goal was to come up with ideas and strategies to make India an IT superpower and one of the largest generators and exporters of software in the world in ten years (i.e. 2008). The task force, consisting of government bureaucrats, ministers, industry officials, IT entrepreneurs, military officers, policy makers, academics and selected Indian IT professionals around the world, solicited suggestions from all interested parties by setting up a web site to post suggestions. The resulting ideas and suggestions were collected and developed into an "Information Technology Action Plan," which consisted of 107 "objectives," categorized under several areas such as "Info-Infrastructure Drive," export targets for IT software and services, strategies for creating IT penetrations and awareness, Citizen IT interfaces, IT in Government, and development of Data Security Systems and Cyber Laws [8]. Objective number 102 specifically called for the establishment of "A National Policy on Information Security, Privacy and Data Protection Act for handling of computerized data shall be framed by the Government within six months." [9].

Despite this high-level proposal, the implementation of some the objectives have been spotty. This is particularly true in the area of developing laws to protect privacy. In its 2003 "Privacy and Human Rights Report," the group Privacy International reported that no legislative action concerning privacy had been taken in India. However, with the aid of the IT Action Plan, as well as pressure from NASSCOM, the software and services industry association, the government of India passed the Information Technology Act in 2000. Thus it becomes evident that in the case of IT-related laws and regulations, the industry has been very active in moving the government forward.

4. Legal protections in the Internet Age

As noted in an earlier section, the Constitution of India, Article 21 provides for privacy protection to its citizens, even though it does not directly do so. Privacy has become included as a one of the protections afforded by the Article through common law precedence set over the years by various rulings.

The Telegraph Act of 1885 provides protection from wiretapping. However, this law has been flouted on several occasions, until the Supreme Court ruled in a 1996 decision in Peoples Union for Civil Liberties (PUCL) vs. The Union of India & Another, that “wiretaps are a ‘serious invasion of an individual's privacy.’” [10]. However, the right to privacy is available and enforceable only against the State. Thus, “if the offender is a private individual then there is no effective remedy except in tort where one can claim damages for intruding in his privacy and no more. Tort itself falls in the gray area.” [11].

In order to keep pace with technology developments, and in keeping with its aim to become a leading provider of software and software services in the word, India enacted its first IT-related laws in the year 2000. The Information Technology Act (2000). The Act provides a comprehensive regulatory environment for electronic commerce, and also addresses computer crime, hacking, damage to computer source code, breach of confidentiality and viewing of pornography. The Act also contained some sections that required cyber-cafés to maintain detailed records of customers’ web browsing habits and provide them to the authorities upon request. However, after a public outcry, these sections were dropped.

Despite the enactment of the IT Act, the tremendous pace of the technology has ensured that privacy can easily be violated. As noted by Agrawal, citing an article by Satyantan Chakrawarty in *India Today*, November 17, 2003, “sometimes the officials transgress their authority and enter the private domain of the people thus infringing their privacy. The Research and Analysis Wing (RAW) had access to bugging, surveillance and counter surveillance equipment. A variety of devices can be used by an investigating agency, like, e-logger, GSM monitor, laser ear, e-mail interceptor, and spy cavities.” [11].

In March 2002 the Indian Parliament passed the Prevention of Terrorism Act (POTA). This was done mostly under the scenario of increasing threat due to terrorist activities over the disputed territory of Kashmir, and under the shadow of the September 11, 2001 terrorist strikes in the US. This Act gave law enforcement sweeping powers to arrest suspected terrorists, intercept communications, and curtail free expression. Critics, including the opposition party at that time, and human rights groups criticized the Act, saying that based on past experience, the law could be used to infringe on people’s privacy and freedom. This, despite the fact that Chapter V of POTA, which deals with the interception of electronic communications, also creates an audit mechanism that includes some provision for judicial review and parliamentary oversight. The over-abiding question is how effective the checks and balances will work in practice.

The above discussion is by no means a complete listing of privacy-related laws enacted in India. But they do provide a good idea of the background and history of privacy and the law in India over the years.

This brings us to the subject of the role of the media, the public and the industry, over the years, in shaping privacy policies and developing cyber laws and privacy laws in India.

5. Privacy laws: the role of the media, industry and the public in a democracy

The IT-industry's premier organization, NASSCOM, has been at the forefront of efforts to bringing India's IT-laws in line with, or at least close to technically advanced nations in Europe and North America. In this, the NASSCOM has been aided by the Indian media organizations who have kept up the public's focus on the risks that data theft and inadequate data protection pose to the Indian public as well as the customers of Indian ITeS companies. The Indian software industry primarily employs members from India's vast middle-class, who also have access to the wide array of news media and news outlets. Thus the efforts of the industry organization, coupled with the democratic processes that allow an open media to disseminate good as well as bad news, and offer critical assessments of the government and the industry, is slowly beginning to raise an awareness of the importance of data privacy among the industry as well as the public employed in the IT sector. Free access to unbiased media, and frequent media exposés have played an important role in educating the public on the value of privacy, while warning the industry leaders of the potential dangers to the IT industry itself, if data was not adequately protected, and privacy was not adequately maintained. This is especially critical to the Indian ITeS industry, as much of its customer base is located in technically advanced countries with sophisticated and well developed laws concerning the protection of data and privacy.

Given this background, NASSCOM has taken a lead in driving public policy concerning data protection and privacy, as well as providing certain directions and standards for IT organizations in India. NASSCOM promotes the concept of "trusted sourcing," which is the term it gives for its efforts in promoting data protection and privacy amongst the Indian IT industry players. The NASSCOM web site has large and comprehensive sections on Information Security and Privacy, Indian Privacy Law and Data Protection. NASSCOM defines "privacy" as "as a combination of maintaining the confidentiality of information and restriction of the use of the information, as authorized by the information owner." [12]. It then provides a list of US and UK laws that pertain to privacy, for the information of Indian IT outsourcing companies.

Over the years, NASSCOM has become particularly concerned about Indian data protection and privacy. This is an area which also seems to be under the cross-hairs of the Indian policy makers, though for a completely different reason. In the post September-2001 world, Indian policy makers have increasingly focused on acquiring surveillance powers and use technologies such as provided by the Internet, as well as other digital forensic tools, to track down terrorists and other extreme elements. This notion of national security is at odds with the notion of privacy that is sought by NASSCOM and other industry groups. In a newspaper article that appeared in May 2005, NASSCOM's president Kiran Karnik expresses his concerns thus: "I feel deeply concerned about the obsession we have with 'security'… which seems to provide a cover-all for anything and everything. It seems to permit the government and its multiple security agencies to do anything from tapping telephones to intercepting mail to seeking identity and sites accessed by cyber cafe users."[13]

Sunil Mehta, Vice-president of NASSCOM, states that "as Internet penetration in India increases, e-governance initiatives grow in reach and more and more 'personal identifiable information (PII)' becomes digitized, many of us are increasingly concerned about privacy and security breaches. I really believe there should be a genuine public debate in this country among all stakeholders around the kind of privacy laws that we, as citizens, really need." [13].

In addition to NASSCOM, the Indian public has also gradually become aware of possible privacy violations that could be caused by technology. The Indian public's access to the Internet has increased, due to the lower costs of computers and Internet access, and due to marketplace pressures as well as governmental policies. At the same time, its awareness and knowledge of use and misuse of personal information has also increased. This has resulted in pressure being exerted on the government to enact and defend laws pertaining to its privacy.

The above statements and emerging public consensus on the issue tend to illustrate the complexities involved with formalizing and legalizing the notion of privacy and privacy protection. While NASSCOM has pioneered and pushed Indian policy makers into enacting IT-related laws, it is also concerned that under the guise of national security, many of the laws, including those pertaining to privacy, made never be implemented in India. NASSCOM has thus become the champion of IT-related laws, including those that protect privacy. The government, on the other hand, is interested in promoting India's IT growth, and in legislating new laws as they pertain to IT misuse. However, there seems to be a hesitation in enacting privacy laws that might restrict its powers in enforcing national security.

In addition to shaping public policy, NASSCOM also provides various guidelines to IT companies on various ways to secure organizational, network and private data in it web site. The aim of this is clearly designed to maintain Indian IT companies' competitive advantage in the global marketplace, and to assure customers that the India ITeS industry is actively taking steps to protect the privacy of its customers' data. By undertaking all of the above activities, NASSCOM seeks to actively promote India's prowess in the global ITeS arena.

6. Analysis and conclusions

In the Indian attempts at establishing high-level data security and privacy standards, we clearly see Christopher Stone's [14] "hand of the marketplace" at work. To elaborate, Christopher Stone, in his book *Where the Law Ends*, states that there are three hands associated with managing a firm to achieve socially desirable behavior. As elucidated by Jeff Smith [15] in a Panel titled "Information Privacy: Management, Marketplace and Legal Challenges," conducted during the ICIS 2004 conference in Washington, D.C., Stone’s “three hands” are: the hand of management, the hand of law, and the hand of marketplace. Smith suggests that managers and executives may not have adequate incentives to shape or follow privacy initiatives. However, that is not the case when the same organization is faced with marketplace issues, such as lack of competitiveness due to lack of privacy standards. In such a situation, such executives would take all the necessary actions needed to shape or influence public policy and get appropriate laws enacted. In doing so, they may sometimes complement or act in opposition to public attitudes that will also play an equally important role in shaping public policy discussion in a democratic environment. The Indian IT industry clearly sees the risks to its well-being and growth that might occur due to compromises in data security and privacy, and is pushing for privacy standards and appropriate laws from the government. However, at the same time, the industry as well as the public balk at the idea of increased security needs that is cited by the government in the implementation of existing Information Technology and privacy laws. Thus, the current Indian scene as regards privacy is hardly clear, especially in the absence of clear-cut privacy laws. What is clear is the overall desire of the Indian IT industry and the Indian government in using the current outsourcing boom to its maximum potential. In doing so, each entity has its own unique reasoning and judgment, which act against each other in some situations, and complement each other in other situations.

Some useful questions for further research in this area could include:

1. The attitudes of Indian IT executives with regards to privacy
2. Cultural studies of Indian software professionals to gain an understanding on their attitudes to privacy.
3. Comparison of Indian privacy laws with US/UK privacy laws.

In conclusion, the answer to the question: “Can we trust the Indians with our data?” is a qualified ‘yes.’ India is definitely making progress in enacting data-privacy and data-protection laws. However, in continuing to do so, the policy makers have to counterbalance national security threats as well as the need to provide a secure environment that is in tune with the needs of its customers from technically advanced nations. In addition, there is a general consensus on the fact that the Indian legal system is currently very slow, and cases take a very long time to prosecute. In order for India to continue on its path to becoming an IT superpower, a conscious effort has to be made to enact appropriate IT laws that specifically apply to privacy and security of data, and to speed up the legal processes pertaining to IT-related cases. This would require a massive effort focused on raising an awareness of, as well as training the policy-makers, judicial system and citizens on the privacy and security issues that technology developments inevitably herald. Further, the political and legal system should be flexible enough to identify and act swiftly on the new and emerging technologies that are sure to come in the future.

References

1. NASSCOM Industry Trends (2003-2004). Para 2. Retrieved April 17, 2006 from http://www.nasscom.org/artdisplay.asp?cat_id=795

2. NASSCOM-McKinsey Report, December 12, 2005. Para 7. Retrieved April 17, 2006 from http://www.nasscom.org/artdisplay.asp?Art_id=4782

3. Jaikumar Vijayan, 2005. "Alleged data theft in India grabs security spotlight," *CIO Asia*, June, 2005. Retrieved April 10, 2006 from http://www.cio-asia.com/ShowPage.aspx?pagetype=2&articleid=1803&pubid=5&issueid=52

4. Rediff.com, April 8, 2005. "Call Center theft may bust India's BPO boom," *Rediff.com.*, Retrieved April 17, 2006 from http://www.rediff.com/money/2005/apr/08bpo.htm

5. Human Rights Watch report, 1999. "Selected Articles of the Indian Constitution." Retrieved on April 17, 2006 from http://www.hrw.org/reports/1999/india/India994-15.htm

6. Agarwala, B.D. 1996. "Right to privacy: A case-by-case development." *Practical Lawyer*, Eastern Book Company. Retrieved on April 17, 2006 from http://www.ebc-india.com/lawyer/articles/96v3a2.htm

7. Subramanian, Ramesh, 2006. "Indian and Information Technology: An Historical and Critical Perspective," in the *Journal of Global Information Technology Management* (JGITM), Vol. 9, No. 4, 2006.

8. Privacy International, 2003. "Privacy and Human Rights Report, 2003," Excerpted from *Information Technology Action Plan, Special Web site on National Taskforce on Information Technology and Software Development, 1998.* Retrieved on April 17, 2006 from http://it-taskforce.nic.in/index.html

9. Privacy International, 2003. "Privacy and Human Rights Report, 2003," Excerpted from *IT for all -2008, Special Web site on National Taskforce on Information Technology and Software Development, 1998.*Retrievd on April 17, 2006 from http://it-taskforce.nic.in/it2008.htm

10. Privacy International, 2003. "Privacy and Human Rights Report – Republic of India, 2003. Para 7. Retrieved April 17, 2006 from http://www.privacyinternational.org/survey/phr2003/countries/india.htm

11. Agrawal, Rachika, 2004. "Privacy and emerging technology: Are Indian laws catching up?" *Lawyers Collective*, February 2004. Retrieved April 17, 2006 from http://www.nwmindia.org/Law/Commentary/privacy.htm

12. NASSCOM, 2006. “Information Security and Privacy – Overview.” Retrieved on April 17, 2006 from http://www.nasscom.org/artdisplay.asp?cat_id=678

13. Indian Express, 2005. “Need for an effective privacy policy,” *Indian Express*, May 30, 2005. Retrieved on April 17, 2006 from http://www.nasscom.org/artdisplay.asp?Art_id=4358

14. Stone, Christopher, 1975. *Where the Law Ends:T he Social Control of Corporate Behavior.* New York: Harper and Row.

15. Yolande Chan,, Mary Culnan, Kathleen Greenaway, Gary Laden and H. Jeff Smith, 2005. “Information Privacy: Management, marketplace, and legal challenges,” *Communications of the Association for Information Systems,* Volume 16, 2005.