THE INDIAN JOURNAL OF LAW AND TECHNOLOGY
Volume 6, 2010

# POLICY-MAKING, TECHNOLOGY AND PRIVACY IN INDIA

*Subhajit Basu*[*]

**ABSTRACT**

*There is a preconceived assumption that privacy laws in India are notoriously weak. This unquestioned assumption is based on a paradigm that does not take into consideration that the conception of privacy in India is influenced by its 'culture of trust.' Unfortunately, rather than looking into the specific societal, political and economic factors triggering the controversy, privacy researchers in the West have constantly varied the meaning and extent of the 'right to privacy' to bolster their argument. This article offers an explanation for why 'umbrella' data privacy legislation similar to the E.U. Data Protection Directive should not be enacted by India. This article further evaluates the argument that one's private sphere is subjective and depends on one's culture, environment and economic condition.*

## I

## INTRODUCTION

This paper critically analyses India's statutory requirements regarding privacy and compares those requirements with the privacy culture established in the West in terms of the texture of the concept of privacy in these distinctly different social and cultural settings. Unfortunately, rather than looking into the specific societal, political, and economic factors triggering the controversy, privacy researchers have constantly varied the meaning and extent of the 'right to privacy.' Most of the definitions of privacy employed are culturally and historically biased in favour of the West and do not take into consideration other socio-historical contexts. What interests me more than the reasoning and the theoretical evidence behind the controversy is the value of looking at how those issues that vex people in the West arise in a different cultural context. Such examinations generate respect and a healthy curiosity.

In addressing privacy as an instrumental notion within social and cultural contexts, we must recognise that people perceive privacy and their 'reasonable expectations' of privacy in a way that has allowed those expectations to change in tandem with ongoing cultural, social and

[*] Senior Lecturer in Cyber Law, School of Law, University of Leeds.

technological changes. While not denying the importance of protecting privacy, this paper presents two plausible explanations for the difference in privacy concerns between India and the Western countries. First, the differences reflect and relate to differences in cultural values (for example the Indian culture of trust) and secondly, the role of privacy rights as embedded in the Indian constitutional tradition.

While critics have argued that privacy laws in India are notoriously weak because of the absence of a comprehensive legislation, the reality is somewhat different. I would argue that this unquestioned assumption is based on a paradigm that does not take into consideration that the conception of privacy in India is quite different from the Western conception of the same right. Firstly, the Indian perception of the word 'privacy' refers to privacy in terms of personal space and subjects.[1] Secondly, even in the West it is not clear what is protected, what is believed to be protected, what is actually protected and what is not protected in terms of privacy. In the course of this paper, I will further argue that one's private sphere is subjective and depends on one's culture, environment and economic condition. The reality of living in a welfare society is that we are living in the era of social reconstruction. It is common for theorists and advocates of privacy to agree that while privacy is an important interest, it must also be balanced against other competing interests. Hence, instead of looking at privacy as a right, I shall refer to privacy as an interest which can be invaded for 'social good.'[2]

My interest in the problem of privacy in the Indian context is motivated by the hysterical reporting of popular mass media in the West on the risk to privacy and data security posed by 'offshore outsourcing' to India. It is undeniable that identity theft and credit card fraud are huge problems

[1] 48% of the subjects in India related privacy to physical, home and living spaces, but only 18% of the subjects in the United States related privacy to these concepts. 89% of the subjects in the United States disagreed with the statement that 'Data security and privacy is not really a problem because I have nothing to hide', but only 21% of the subjects in India disagreed with the above statement. Regarding privacy issues in relation to technology, a minority (21%) of the subjects in India expressed concern about keeping computerised information secure, but 79% of the subjects in the United States expressed such a concern. While responding to the above question, 25% of the subjects in the United States expressed concern about identity theft, but the topic remained unaddressed by the subjects in India. *See* PONNURANGAM KUMARAGURU ET AL., PRIVACY PERCEPTIONS IN INDIA AND THE UNITED STATES: AN INTERVIEW STUDY (2005), *available at* http://www.cs.cmu.edu/~ponguru/tprc_2005_pk_lc_en.pdf.

[2] The Government of Australia has recently relaxed privacy laws to pass on personal information about half a million foreign students across the country to the police in order to help them investigate whether the recent attacks on foreign students, including Indian students, were racially motivated. According to Australian Privacy Commissioner Karen Curtis, the release of students' names and ages, held by the Department of Immigration, was a one-off decision in the national interest. *Oz relaxes laws to pass details of foreign students to police*, ECON. TIMES, May 20, 2010, *available at* http://economictimes.indiatimes.com/news/politics/nation/Oz-relaxes-laws-to-pass-details-of-foreign-students-to-police/articleshow/5953900.cms.

globally; however, there is no evidence, to suggest that consumer data is at any greater risk in India than in the UK[3] or the US,[4] nor is there any evidence to prove that consumers in highly regulated countries trust the companies collecting their personal data,[5] hence it is unjustified to stigmatize one particular country or group of countries unnecessarily. The intention of this article then is to offer an explanation for why India's conception of privacy is dominated by the public-private dichotomy and has implicitly or explicitly affected the agenda for privacy theory by placing some issues in the limelight and others backstage.

## II

## PRIVACY EFFICACY

Social patterns and values today are too diverse, decentralised, and purposefully different to provide a foundation for general rules of discourse at the level of specificity required for the protection of privacy. This does not imply that a legal concept of privacy should be disregarded; instead, protection can be defined as specifically or as generally as the legislature chooses by taking into consideration the cultural context and allow its contours to fit within the social and economic conditions. It is important that we explore these foundations for the purposes of identifying the assumptions, assessing its justifications, and analysing the paradoxical effects of India's privacy policies.

The idea of privacy is intimately connected with the conception of liberty, justice, human dignity, individuality and family life. Although the concept of privacy is a longstanding phenomenon, codification of privacy as a right is rather new. Further, as societies go through a fundamental transformation, it also creates the need for re-conceptualising the right to privacy. The question arises in terms of how far it should be protected and against what? Most scholars tend to define privacy within the confines of their specific research. For example, privacy as the 'right to be let

---

[3] The UK's Information Commissioner's Office reports that nearly 100 data breaches were reported in the three months since October 2008. The number of data breaches has increased by almost 36% as compared to the previous year – 376 data breaches at the end of January 2009 as compared to 277 data breaches at the end of October 2008. It thus appears that personal information is now lost more than once a day on average. *See* Press Release, Information Commissioner's Office, Data breaches reported to ICO (Feb. 9, 2009), *available at* http://www.ico.gov.uk/upload/documents/pressreleases/2009/data_breaches_ico_statement20090209.pdf; *see also* Richard Thomas, UK Information Commissioner, Speech to the RSA Conference Europe (Oct. 29, 2008), *available at* http://www.ico.gov.uk/upload/documents/pressreleases/2008/rsa_speech_oct08_final.pdf.

[4] *See* Joseph Cannataci & Jeanne Bonnici, *The UK 2007-2008 Data Protection Fiasco: Moving on from bad policy and bad law?*, 23 INT'L REV. L. COMPUTERS AND TECHNOLOGY 47 (2009).

[5] *See* Press Release, IBM, E-businesses exhibiting privacy leadership get the sale, according to new IBM consumer study on privacy (Nov. 8, 1999), *available at* http://www-03.ibm.com/press/us/en/pressrelease/1979.wss.

alone' is a rather simple concept and cannot be used in a meaningful way. Such a narrowly constructed conception of privacy in obvious ways is restricted in its utility. Gavison argues that, 'not letting people alone' cannot readily be described as an invasion of privacy.[6] I argue that what counts as a right to privacy, then, has the potential of having important consequences on a variety of scales. Hence, inevitably, the demands of the modern society and technological changes require a redefinition of the right to privacy.

Does everybody in society get equal protection in terms of privacy and how much privacy is desirable? Every individual should have the same claim to privacy. Thus, one individual's exercise of privacy must submit to the equal claim of every other individual to the same exercise. However, in reality, this does entail some loss of privacy for everybody. Gavison argues that there is a loss of privacy when others obtain information about an individual, pay attention to him or her, or gain access to him or her. She suggests that the concept of privacy consists of a complex combination of three elements – secrecy, anonymity and solitude.[7] While these elements are independent of each other, they are also related. Privacy therefore consists of the individual's control over access to, and information about, himself or herself.[8] An individual who chooses to disclose certain aspects of his or her private life cannot experience a loss of privacy on the ground that others gain access to him or her. On the contrary, if the individual chooses not to allow others to gain access to himself or herself, or his or her personal information, then any intrusion into his or her private affairs or a disclosure of his or her personal information would violate his or her right of privacy. Therefore, the variation in the quality of privacy is dependent on the extent and frequency with which an individual is 'exposed' to the public. It seems reasonable to suppose that, as with other social values, some inequality in the distribution of privacy does exist.[9]

It is with this purpose that I distinguish 'informational privacy' from 'decisional privacy.' The focus of decisional privacy is on freedom from interference when making certain fundamental decisions. In contrast, informational privacy is concerned with the use, transfer, and processing of personal data generated in daily life. "The extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others'

---

[6] Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 437 (1980).
[7] *Id.* at 428.
[8] James Rachels, *Why Privacy is Important*, 4 PHIL. & PUB. AFF. 323, 326 (1975).
[9] COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 35 (2003).

attention."[10] This approach has been criticised on the ground that if a loss of privacy occurs whenever any information about an individual becomes known, then the concept of privacy loses its intuitive meaning. Such a proposition leads to the awkward result that any loss of the solitude of, or information about, an individual becomes a loss of privacy.[11]

Contrary to approaches like Gavison's, Wacks[12] argues that a limiting or controlling factor is required. He points out that although focusing attention upon an individual or intruding upon his solitude is inherently objectionable in its own right, our concern for the individual's privacy in these circumstances is strongest when the person is engaging in activities that we would normally consider private. He suggests that the protection afforded by the law of privacy should be limited to information "which relates to the individual and which it would be reasonable to expect him to regard as intimate or sensitive and therefore to want to withhold or at least to restrict its collection, use, or circulation."[13] If the right to privacy would be recognised by law, it would extend only over a limited, conventionally designated, area of information,[14] "symbolic of the whole institution of privacy."[15] Hence, it can be argued that access to personal information is a necessary but not sufficient condition for it to be defined as falling within the scope of privacy. What is further required is that the information must be of an intimate and sensitive nature, such as information about a person's sexual proclivities, but the content may also differ considerably from society to society.

## III

## PRIVACY IN INDIA'S CULTURAL PERSPECTIVE

The existence of multiple cultures and philosophies prompts questions regarding appropriateness, hegemonic relations, and privileging one culture over another. Before the debate can begin, we need to understand that each nation has a distinctive, influential, and describable culture;[16] hence, each country, from its own unique background, determines the ways in which its citizens express

---

[10] *Supra* note 6.

[11] RAYMOND WACKS, PERSONAL INFORMATION: PRIVACY AND THE LAW 15-18 (Clarendon Press 2003) (1993).

[12] *Id.* at 26.

[13] *Id.* at 26.

[14] Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW & PHIL. 559 (1998).

[15] Charles Fried, *Privacy,* 77 YALE L.J. 493 (1968).

[16] Culture is "the interactive aggregate of common characteristics that influences a human group's response to its environment. Culture determines the identity of a human group in the same way as personality determines the identity of an individual." *See* GEERT HOFSTEDE, CULTURE'S CONSEQUENCES: INTERNATIONAL DIFFERENCES IN WORK-RELATED VALUES 25-26 (1980).

and understand the same concept.[17] What makes Indian culture special is the concept of the autonomous non-distinctive individual not living within society. When it comes to the 'man-in-society,' the Indian view is not unique. Indeed, the view is a prototypical and lucid expression of a widespread mode of social thought,[18] but it does diverge quite considerably from the 'natural man' tradition of Western social thought.[19] The Western "autonomous individual imagines the incredible, that he lives within an inviolate protected region (the extended boundaries of the self) where he is 'free to choose'."[20] I will contrast this with the alternate conception, the holistic culture of India, which seems to embrace a socio-centric conception of the relationship of the individual with society. According to Hofstede,[21] India is a collectivist society with a lower Individualism Index (IDV)[22] and a higher Power Distance Index (PDI)[23] as compared to the UK or the US, which are individualist societies with higher[24] IDV where an individual's importance is at least equal to, if not greater than, the importance of the collectivity. Hofstede has shown that individuals in collectivist societies have more faith in other people than those in individualist societies.[25]

A country's cultural values are known to affect a population's attitudes toward privacy and are associated marginally with its regulatory approach.[26] What then are the influences of cultural specificity on privacy? Western societies came to view privacy as an important value that gave rise to a privacy interest or right recognised by law or social convention.[27] Unsurprisingly, Indian cultural values also play a significant role in shaping attitudes about privacy. It is in the interest of the Indian society that both the individual rights aspect of privacy as well as the social value of

---

[17] *Id.* at 25-27.

[18] *See* D. W. Murray, *What is the Western Concept of the Self? On Forgetting David Hume*, 21 ETHOS 3 (1993).

[19] Richard A. Shweder & Edmund J. Bourne, *Does the Concept of the Person Vary Cross-Culturally?*, *in* CULTURE THEORY: ESSAYS ON MIND, SELF, AND EMOTION 158-199 (Richard A. Shweder & Robert A. LeVine eds., 1984).

[20] *Id.* at 182.

[21] Hofstede developed a number of cultural values indices to measure cultural differences between societies. He identified five distinct dimensions of human behavior that characterize a culture: (1) power distance, (2) uncertainty avoidance, (3) individualism/collectivism, (4) masculinity/femininity, and (5) long-term or short-term orientation. GEERT HOFSTEDE, CULTURE'S CONSEQUENCES: COMPARING VALUES, BEHAVIOURS, INSTITUTIONS, AND ORGANIZATIONS ACROSS NATIONS 79 (2001).

[22] The Individualism Index (IDV) measures the extent to which a society tends to emphasize individual rights as compared to collective goals. *Id.* at 79.

[23] 'Power distance' is defined as the way in which a culture approaches and accepts inequality in status, prestige, wealth and power. *Supra* note 21.

[24] *Supra* note 21.

[25] *Supra* note 21.

[26] *See* Sandra J. Milberg et al., *Information Privacy: Corporate Management and National Regulation*, 11 ORG. SCI. 35, 39 (2000).

[27] Alan F. Westin, *Social and Political Dimensions of Privacy*, 59 J. SOC. ISSUES 431 (2003).

privacy is preserved. However, the degree of need for such preservation would vary from individual to individual and would make it highly subjective. While it is a common practice in the UK for general practitioners (GPs) to not discuss patient information relating to the wife with her husband, such discussion is quite common in India, where GPs regularly discuss such issues with the husband or other members of the family. Interestingly, I sometimes find myself contradicting my own thoughts because I am torn between the dichotomy of the Western conception of total control over information and the Indian culture of trust. The result is two worlds with clear rules. However, problems arise because these diverse cultures are interacting with each other, yet each culture is retaining its own set of values and beliefs.

Are any aspects of life inherently private and not just conventionally so? As discussed in the previous section, one of the interests most commonly associated with privacy is the interest in controlling access to, and dissemination of, information about oneself. Hence, not surprisingly, in India and probably in every other place in the world, people recognise that certain types of information about oneself are privileged. However, in India, the people's perception about 'privacy' is predominantly associated with 'secrecy' and 'personal space' and how people relate to, communicate and share each other's professional, familial and personal information but it is not about the economic value of that information. Indeed, the concern for 'bodily privacy' is amongst the most ancient and deeply traditional concerns of both Hindu and Muslim cultures. In *Ganeshi Lal v. Rasool Fatima*,[28] the court found that Indian women have always been protective of their privacy in their homes. It is the archetypal private space. Privacy inside the house is a right of every woman and much more so for a woman who has inhibitions by custom or religious notions against appearing in public and keeps herself in seclusion by observing 'purdah.'[29] In *Basai v. Hasan Raza Khan*,[30] the court recognised 'purdah' as the basis of this right and held that it entitled the owner of one property to compel the owner of another to modify the design or architecture of his property so that the woman residing in the dominant tenements could be kept in 'purdah.' According to the court, the right is based on 'natural modesty or human morality.' The court, however, held that the customary right to privacy can be claimed only in respect of apartments which are generally occupied and used by females and does not extend to apartments ordinarily used by males, the basis of the customary right of privacy being the 'purdah' system which was

[28] A.I.R. 1977 All. 118 (India).
[29] 'Purdah' literally means curtain. It is the practice of preventing women from being seen by men. This takes two forms: physical segregation of the sexes, and the requirement for women to cover their bodies and conceal their form. Purdah exists in various forms in the Islamic world and amongst Hindu women in some parts of India.
[30] A.I.R. 1963 All. 340 (India).

confined to the protection of 'purdanashin' women and those parts of a house which were ordinarily occupied by females.

It can be further argued that custom once established does not extend only to women who are in the habit of observing 'purdah,' but all women are entitled to this specific degree of privacy. Although it is equally true that the right of privacy cannot be extended to an oppressive length, a variety of social, economic and technological changes in India, have, over the years, seemed to widen the arena within which the presumption of a right to privacy ought to operate. Over this period, the area within which private activities can take place has also been extended beyond the home. In the recent *Naz Foundation* case, the Delhi High Court held that the right to privacy protects a "private space in which man may become and remain himself."[31] The judges predicated their application of the right to privacy in this case with a discussion of the concept of 'dignity' and its presence in the Indian Constitution. The court observed that "at its least, it is clear that the constitutional protection of dignity requires us to acknowledge the value and worth of all individuals as members of our society. It recognizes a person as a free being who develops his or her body and mind as he or she sees fit. At the root of dignity are the autonomy of the private will and a person's freedom of choice and action."[32] The decision articulates a unique, non-spatial and portable understanding of privacy that extends beyond 'place' into 'person.' It is potently clear that the Indian conception of privacy is dominated by factors such as the rights of the family, the 'purdah' observed by women and the belief that such intrusion affects the modesty, dignity or decency of a person. However, it is not sufficient in conceptual terms to treat an invasion of privacy as an affront to human dignity alone, as it is possible that an individual's dignity could be offended without his privacy being invaded.

Interestingly, similar findings regarding public perception of privacy were reported in the two surveys published by the School of Computer Science at Carnegie Mellon University.[33] Both surveys are quite revealing in the sense that they vividly underline the great gap that separates the Western perception of privacy and the predominant perception in India. The two surveys found

---

[31] Naz Foundation v. Government of N.C.T. of Delhi & Ors., 160 (2009) D.L.T. 277 (India) (*Per* A. P. Shah, C.J. & S. Muralidhar, J.). The Delhi High Court decided to strike down provisions that criminalised consensual homosexual sexual conduct on the grounds of invasion of privacy.

[32] *Id.* at ¶ 26.

[33] *See* Ponnurangam Kumaraguru & Lorrie F. Cranor, *Privacy in India: Attitudes and Awareness*, *in* PROCEEDINGS OF THE 2005 WORKSHOP ON PRIVACY ENHANCING TECHNOLOGIES (PET 2005: 30 MAY - 1 JUNE 2005, DUBROVNIK, CROATIA), *available at* http://lorrie.cranor.org/pubs/PET_2005.html; *see also supra* note 1.

that typical responses by Indians when asked about privacy were 'privacy for me is my personal territory' and 'personal privacy.'[34] However, the surveys also do not show that privacy is 'less valued' in Indian culture. These surveys completely undermine a familiar canard about non-Western societies;[35] that they do not ascribe the same value that Western societies do to privacy.[36] It confirms that Indians are more concerned with a different dimension of privacy and so ascribe a greater value to protecting the concerns that fall under the same.[37] It further re-emphasises that privacy is a highly subjective value. Public policy and law can only establish rules, principles and procedures if and when the same are required or demanded (e.g. if there are concerns about information privacy then governments can become more involved because individuals are more likely to call for stronger privacy laws) but it is also up to individuals to assert their own privacy interests and claims. Hence, there is a positive statistical relationship between nationality, privacy concerns and privacy regulations.[38]

Ethical relativism postulates that "morality is relative to the norms of one's culture"[39] and that "whether an action is right or wrong depends on the moral norms of the society in which it is practiced."[40] We cannot apply a universal code of ethics and laws across the world given our different cultures and beliefs. The overriding question is which set of ethics and beliefs should be

---

[34] With regard to cultural prescriptions and privacy, Kumaraguru & Cranor refer to the lack of an explicit privacy concern be it amongst family members running a family business or in the work place. There exists a certain amount of naiveté about databases of personal information traded and sold between trading companies. *Id.*

[35] For example, the concept of privacy in Thailand is 'collective' and different from the more 'individual' Western conception. Buddhism, which is practiced by most people in Thailand, does not recognize human beings as possessing inherent rights endowed at birth in the sense of human rights such as the right to privacy. So, the word 'privacy' has different cultural understandings. *See* Krisana Kitiyadisai, *Privacy Rights and Protection: Foreign Values in Modern Thai Context*, 7 ETHICS & INFO. TECH. 17 (2005). From a Chinese perspective, privacy is also not seen as an 'intrinsic good' but as an 'instrumental good', meaning that the Chinese do not view privacy as essential, although they consider the concept to be important. *See* Lü Yao-Huai, *Privacy and Data Privacy Issues in Contemporary China*, 7 ETHICS & INFO. TECH. 7 (2005).

[36] *See* Martha C. Nussbaum, *Is Privacy Bad for Women? What the Indian Constitutional Tradition can teach about sex equality*, 25 BOSTON REV. 42 (2000).

[37] Debate about policies, community expectations, industry codes and legislation has primarily addressed data collection/handling by government agencies rather than the private sector. In particular, it has centred on political surveillance and censorship, reflecting the public outlook about civil society and individual rights.

[38] Milberg and Westin found that countries with either 'no privacy regulations,' or the strictest model of privacy regulations were associated with significantly lower information privacy concerns, and countries with moderate regulatory structures were associated with higher aggregate levels of concern. *See* ALAN WESTIN, PRIVACY AND FREEDOM (1967); *see also* Sandra J. Milberg et al., *Values, Personal Information Privacy, and Regulatory Approaches*, 38 COMM. OF THE ACM 67 (1995).

[39] Claire Andre & Manuel Velasquez, *Ethical Relativism*, 5 ISSUES IN ETHICS (MARKKULA CENTRE FOR APPLIED ETHICS) (1992), *available at* http://www.scu.edu/ethics/publications/iie/v5n2/relativism.html.

[40] *Id.*

used to set rules and laws? History itself is littered with examples of 'uninvited cultural invasion and overthrow,'[41] where values and assumptions were adopted with little questioning.

What results from this discussion, I contend, is not a choice of one over the other but rather a dualism. To me, a more effective argument for the cultural relativity of privacy conceptions would be structured differently. Any reasonably developed culture has a basic understanding of privacy based around a 'minimal conception.'[42] It is important to note here that this 'minimal conception' is shared by all cultures. What is then required is multiple matching between these variations in cultures and their respective privacy conceptions.[43] Hence, the policy need not be common, but neither should it be singular, it should rather be a conjunction of contexts that requires the norms of each context to be respected and protected from homogenisation.

What has been the influence of the 'technological culture' of information technology? Information technology has managed to streamline and amplify the collection and analysis of data as well as its use in decision-making. It is true that because of this we are now producing, processing, storing, automatically sorting, extracting and comparing vast amount of data like never before.[44] It appears to provide a panacea of observation, analysis, prediction, and control for those who wish to reduce uncertainty and unpredictability. As I have mentioned before, in an information society, those who send information and those who filter information have economic power and also have the power to influence and shape privacy and probably will ultimately control the privacy of individuals. But it has also created vulnerability. In the case of India, at the present moment, it seems that this vulnerability is the lack of clarity regarding the classification of information, which is making the management of information much more complicated. In the next section, I will discuss if it is in the economic interest of India to adopt a definitive privacy policy, specifically in the context where privacy is perceived to be threatened by new technologies.[45] The focus of the section is on the intersection of privacy and economics.

---

[41] TREVOR HAYWOOD, INFO-RICH INFO-POOR: ACCESS AND EXCHANGE IN THE GLOBAL INFORMATION SOCIETY 131 (1995).

[42] Masahiko Mizutani et al., *The Internet and Japanese Conception of Privacy*, 6 ETHICS & INFO. TECH. 121, 121-128 (2004).

[43] Different cultures will receive and interpret information differently regardless of the universal concepts which all people share. The same information will not produce the same understanding.

[44] A basic list of technologies that have the potential to impact privacy are: radio frequency identification, smart cards, location detection technologies including G.P.S., data mining technologies, surveillance technologies and biometrics.

[45] India's outsourcing industry is expected to earn revenues amounting to $50 billion by 2012. It is also expected to provide direct employment to 2 million workers by 2012. The outsourcing industry in India has grown at more than

## IV

## PRIVACY IN INFORMATION SOCIETY: ECONOMIC CULTURE

Cultures are not independent of economic and technological forces. The interplay between technological development and cultural curiosity is helping to define the information society. The information economy continues to drive Indian commerce.[46] Indian outsourcing and information technology companies have created hundreds of thousands of jobs in India,[47] the industry has completely revolutionised how consumers and businesses interact, transact and use information. Hence, the dilemma for India, which has a substantial interest in the development of information industries, is whether the country can completely ignore the Western, particularly the European, demand for specific data privacy legislation. Usually this dilemma is never stated so obviously but its existence is accepted nonetheless.

The internet is transforming critical sectors of the global economy and society, such as health care, energy, education, the arts and political life. In all these sectors, proper use of personal information can play a critical, value-adding role, so establishing trust and assuring flexibility is vital. The economic significance of privacy in an information society is dependent on how much people value their privacy. The earliest economic analyses of privacy focused on the efficiency of markets for personal information. Almost all developed countries have grappled with the trade-off between open access to information which enables economic efficiency and an individual's right to privacy. My objective here is to briefly evaluate the utility of allocating the value of personal information. Laudon argues that market-oriented mechanisms based on individual ownership of personal data could enhance personal data protection.[48] If 'personal data markets' were allowed to function more effectively, there would be less privacy invasion.

Under the traditional economic model, competitive market forces will generally deliver an economically efficient outcome. Hence, an efficient amount of information sharing will occur up to the point where the economic benefits of information sharing are balanced against the associated costs. Specifically, if the economic value created by information sharing exceeds the value derived from privacy, theory maintains that the economically efficient outcome would be to share information. In contrast, if the economic value generated by private parties from access to

---

30% a year for five years since 2003. *India's outsourcing revenue to hit $50 bn*, FIN. EXPRESS, Jan. 29, 2008, *available at* http://www.financialexpress.com/news/indias-outsourcing-revenue-to-hit-50-bn/266661.

[46] *Id.*

[47] *Supra* note 45.

[48] Kenneth C. Laudon, *Markets and Privacy*, 39 COMM. OF THE ACM 103 (1996).

personal information does not exceed the individual benefit from privacy, then economic efficiency dictates that information is not be shared.[49] In other words, individuals will provide personal information as long as they perceive that adequate benefits shall be received in return – i.e. benefits which exceed the perceived risks of information disclosure.[50] So long as individuals undervalue their personal information relative to its market value, there will be a buyer for it in today's information hungry economy.[51] This perception is important from a developing country perspective because there is a direct relationship between micro-economics, the use of personal data and the increase in contribution to the Gross Domestic Product (GDP), national competitiveness and economic growth; this means that governments should evaluate the practical implications for businesses before introducing stringent privacy regulations protecting personal information.

Milberg found a significant and positive relationship between concerns about information privacy and the level of government involvement in the regulation of privacy.[52] There can be various situations involving both consequential and direct externalities where the commitment to protect privacy increases welfare. Specifically, certain analyses of behaviour-based price discrimination in competitive settings show that businesses may benefit from the privacy of personal information.[53] It is worth remembering in this respect that the economic analysis of consequential externalities suggests that whether and how privacy increases welfare depends on the particular circumstances.[54] The economic analysis of consequential externalities suggests that whether and how privacy increases welfare depends on the particular circumstances. Clearly, a free market for personal information will not provide an economically efficient outcome. Hence, from an economic point of view, the question is whether privacy regulation is more likely to increase welfare in the context of non-productive information as compared to productive information. Understanding how the private sector uses personal information can reveal how policies and regulations to protect privacy can be properly tailored; this means that the contentious debate about privacy regulation may have

---

[49] *See* Hal R. Varian, *Theory of Markets and Privacy*, *in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (1997), *available at* http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm.

[50] *See* Alessandro Acquisti & Jens Grossklags, *Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyberbolic Discounting*, *in* THE ECONOMICS OF INFORMATION SECURITY 5 (J. Camp & R. Lewis eds., 2004), *available at* http://www.heinz.cmu.edu/~acquisti/papers/acquisti_grossklags_eis_refs.pdf.

[51] *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1465 (2000).

[52] *Supra* note 26, at 39-57.

[53] Drew Fudenberg & J. Miguel Villas-Boas, *Behaviour-Based Price Discrimination and Customer Recognition* (2005), *available at* http://www.haas.berkeley.edu/~market/PAPERS/VILLAS/surveypaper.pdf.

[54] K. L. Hui & I. P. L. Png, *The Economics of Privacy*, *in* HANDBOOKS IN INFORMATION SYSTEMS (Terrence Hendershott ed., 2006).

been misdirected. Finally, it is undeniable that economic diplomacy has now become pivotal part of Indian foreign policy, but economic policy cannot be detached from the socio-political and cultural reality of the country.

## V

## INDIAN JUDICIAL RECOGNITION OF RIGHT TO PRIVACY

Despite pressure from internal and external sources, India has traditionally shown a general unwillingness to adopt data privacy laws.[55] I have stated before that there is a significant and positive relationship between concerns about privacy and the level of government involvement in the regulation of privacy.[56] Thus, differences in political systems and legislation in various countries can be interpreted as consequences of societal value differences and the degree to which members of a society look to the government to remedy social issues.[57] In the United States[58] and, until recently, Canada and Australia, privacy regulation has tended to be targeted and sector specific, and to be aimed mainly at the public sector. This sectoral or voluntary approach contrasts with the omnibus approach, to both the public and private sectors, used by the European Union. The right to privacy in India is a peculiar blend of constitutional, customary and common law rights scattered across various legal fields. As a customary right, it is treated as an easement. As a part of the constitutional right to life and liberty, it is considered to be an illustration of the prerogative development of human rights and basic freedoms.

The analysis made earlier in the article emphasises that India's history has not been plagued by privacy abuses and identity theft. It is true that there is a positive association between the level of privacy concern and the level of governmental involvement in the management of privacy but I am inclined to argue here, however, that India's recent general reluctance to legislate for data privacy protection may be deeply rooted in its colonial past. A country's 'legal origin' significantly affects the subsequent evolution of its legal rules. Due to the greater constitutional independence of the judiciary in 'common law' legal systems, such legal systems are thought to exhibit both a greater

[55] At the time of writing this article, India still has not adopted a legislation which explicitly governs the protection of personal data. Data privacy protection was discussed in the late 1990s as part of the formal discussions regarding the provisions to be included in the proposed information technology legislation, but the Information Technology Act, 2000 did not include provisions in relation to data privacy.

[56] *Supra* note 26, at 35-57; Milberg et al., *supra* note 38, at 65-74.

[57] *Supra* note 26, at 35-57.

[58] The US privacy framework is composed of sectoral laws combined with constitutional, statutory, regulatory and common law protections, in addition to industry self-regulation. Sectoral laws govern the handling of personal data considered to be most sensitive in nature.

degree of adaptability than 'civil law' legal systems through their greater reliance on 'bottom up' rule-making by the judiciary as opposed to 'top-down' codifications, and a lesser degree of susceptibility to corrosion by rent-seeking politicians and bureaucrats.[59] Although India is described as a common law country having inherited a common law legal system from the UK, many of its laws were, in fact, codified during colonial rule, which was driven by an agenda of distrust that resulted in an array of rules and regulations that were almost impossible to uphold. In post-independence India, these were then overlaid with more legislation when the government implemented a socialist reform agenda encompassing all areas of commercial activity resulting in an obstructive bureaucracy[60] and relentless overregulation. The legal system that India inherited from the colonial era suffers from three defects – delay, cost and glorious uncertainty in the final outcome of any litigation. It is a maze of complex procedures together with a multiplicity of laws. In the wake of this pattern, businesses in the private sector had to wait months or even years for a response to their requests for government approval of entrepreneurial projects at many times waiting in vain.[61] It was not until the 1990s that this overly-stifling quagmire of excessive government control started to get dismantled, and since then, there have been rapid and far-reaching law reforms.[62]

The repressive environment which dates from the colonisation of India and has lasted through independence has caused an understandable fear of government regulation.[63] Furthermore, the nature of coalition politics in India, coupled with a very active judicial review process, means that enacting legislation is a slow and erratic process. Hence, the scepticism about legislation protecting data privacy is understandable. It has also provoked the questions of whether and to what extent, if at all, the current constitutional tradition provides privacy in India. Should it be supplemented to

---

[59] John Armour & Priya Lele, *Law, Finance, and Politics: The Case of India* (Eur. Corp. Governance Inst. (ECGI), Law Working Paper No. 107, 2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1116608.

[60] Indrajit Basu, *India tries to root out bureaucratic corruption*, ASIA TIMES, Oct. 9, 2003, *available at* http://www.atimes.com/atimes/South_Asia/EH07Df01.html.

[61] GURCHARAN DAS, INDIA UNBOUND 216-218 (2002).

[62] The liberalising New Economic Policy of 1991 lead to a dramatic reconfiguration of the Indian economy. The motivating idea was to move from an economy controlled and planned by the state to one in which the private sector was to have a significant role, competition was to be encouraged, market-oriented mechanisms were to be developed, and government intervention was to be limited to the extent justifiably required. *See* JAGDISH N. BHAGWATI, INDIA IN TRANSITION: FREEING THE ECONOMY (1993); *see also* A. Panagariya, *India in the 1980s and 1990s: A Triumph of Reforms* (International Monetary Fund (IMF), Working Paper No. 3, 2004).

[63] In India, there is no sunset provision for statutes, and so, unnecessary statutes remain on the statute books till they are repealed. Some of these dysfunctional legislations have been repealed on the basis of the reports of the Law Commission of India which have been accepted by the Government of India. But several such statutes including some statutes from the British period are still cluttering the statute books.

manage privacy in the information society? Or is there a need for more radical changes in Indian law and policy to effectively address privacy concerns?

There is a substantial debate regarding whether a 'right to privacy' exists in India, how such a right is derived philosophically, and the extent to which such a right, if it does exist, is bounded. However, we should be asking an altogether different question: if we were to deny that people have a right to privacy, what would be the impact of this denial on the values that the Indian Constitution was designed to protect? Certainly, the Indian courts did not recognise any natural right to privacy and believed that such a right can be acquired only as a customary easement.[64] Indian courts have long acknowledged the relationship between privacy and information about persons, and have argued for limits on allowable practices of information gathering, analysing, and sharing as a means of protecting privacy, but all their efforts have primarily applied to intimate and sensitive information. How far have the Indian courts taken the fledgling right to privacy? Indian judges like the English judges have explicitly invoked such a right, though without taking the final step of creating a new legal right. The Allahabad High Court in *Nihal Chand v. Bhawan Dei*[65] had first recognised the independent existence of the right to privacy:

> the right to privacy based on social custom is different from a right to privacy based on natural modesty and human morality, the later is not confined to any class, creed, colour or race and it is a birth right of any human being and is sacred and should be observed.

The Indian Constitution does not expressly recognise the right to privacy but there is a strong belief that the Indian Constitution contains certain rights other than those that are expressly mentioned in its text. To establish the presence of such a right, it must be shown that the right in question is an integral part of an enumerated right upon which its existence depends. The rationale behind this formulation is simply that the enumerated right would be meaningless without providing for certain other rights by implication. Hence, the Supreme Court of India[66] accepted in 1964 that a right of privacy[67] is implicit in the Constitution under Article 21, which states, "no person shall be deprived of his life or personal liberty except according to procedure

---

[64] C. Krishna Murthy v. U. Rajlingam, A.I.R. 1980 A.P. 69 (India), ¶ 8.
[65] A.I.R. 1935 All. 1002 (India).
[66] India's independent judiciary, with the Supreme Court at the apex, has been a key feature of India's democracy throughout its existence. The role of the Supreme Court as the protector of individual rights is guaranteed under the Constitution of India. Basic individual rights are given constitutional protection as 'fundamental rights'. *See* INDIA CONST. arts. 12-35.
[67] Kharak Singh v. State of U.P., (1964) 1 S.C.R. 332 (India).

established by law."[68] The Supreme Court equated 'personal liberty' with 'privacy,' and observed that the concept of liberty in Article 21 was comprehensive enough to include privacy and that "nothing is more deleterious to a man's physical happiness and health than a calculated interference with his privacy."[69] On the basis of this provision, the Supreme Court held that "those who feel called upon to deprive other persons of their personal liberty in the discharge of what they conceive to be their duty must strictly and scrupulously observe the forms and rules of the law."[70] In the case of *People's Union for Civil Liberties v. Union of India*,[71] the Supreme Court held that the right to life and personal liberty under Article 21 includes the right to privacy and so improper telephone tapping violates Article 21.

At the time of the drafting of the Indian Constitution, the home was seen as the central locus of intimate activities, and hence as the place where the intervention of the government needed the strongest justification. Indian courts have thus interpreted the right to privacy as an implied fundamental right against state action. The perception of privacy as a fundamental right also changes depending on the person concerned and the context in which this right is being exercised. It is not viewed as an 'absolute' right, nor does it address 'information privacy.'[72] Indian case studies[73] also illustrate a significant tension between the contours of the right to privacy as against other rights and interests.[74] Even in its constitutional context, the meaning of privacy and how far the right to privacy extends remains unclear.[75] Somewhat unfortunately, the constitutional right to

---

[68] Madhavi Divan, *The Right to Privacy in the Age of Information and Communications*, 4 SCC (J.) 12 (2002).

[69] *Supra* note 67.

[70] *Supra* note 67; Gobind v. State of M.P., (1975) 2 S.C.C. 148 (India); State v. Charulata Joshi, (1999) 4 S.C.C. 65 (India).

[71] A.I.R. 1997 S.C. 568 (India).

[72] In the case of *State of Maharashtra v. Madhulkar Narain,* A.I.R. 1991 S.C. 207 (India), it was held that the 'right to privacy' is available even to a woman of easy virtue.

[73] This argument is supported by two widely debated cases of invasion of privacy in India. The first one is the DPS MMS scandal case in which Baazee.com CEO and Indian-born US citizen Avnish Bajaj was sent to jail for six days by a Delhi court. The focus of this case was not on the intrusion of privacy but the illegal distribution of the MMS clip on net. The police claimed that Baazee.com had listed the MMS clip on its website for sale and that the CEO did not make any efforts to remove it until prodded. The second case involved stealth video footage of an actor, captured by a media agency, invading privacy in the process and the actor found little recourse in law apart from being able to file a defamation suit.

[74] The Supreme Court has held that intrusions into privacy can be permitted and justified using legislative provisions, administrative/executive orders, and judicial orders. The court can compare the reasonableness and proportionality of the intrusion vis-à-vis the purpose of the intrusion. However, the Supreme Court did not take into account the possibility that the procedure established by law in India might be unjust or unreasonable. *See supra* note 67; *see also* Gobind v. State of M.P. (1975) 2 S.C.C. 148 (India); *see also* State v. Charulata Joshi, (1999) 4 S.C.C. 65 (India).

[75] In *M. P. Sharma v. Satish Chandra*, A.I.R. 1954 S.C. 300 (India), the Supreme Court held that the power of search and seizure does not violate the right to privacy because it is in the interest of the State. However, in *Menaka Gandhi v.*

privacy, although recognised in India and based on the comparative theoretical evaluation of Western and Indian legal systems for protecting privacy, is far more restrictive. It also cannot be denied that there is an uncertainty about the conceptual basis of privacy. However, I argue that although it is evident from the examination of the constitutional position and the history of the right to privacy in India that the right must be made subservient to national interest and national security at all times, recent Supreme Court decisions reflect conceptions of cultural and technological change and economic need.

Informational privacy, understood as data protection in the digital environment, is seen as an economic issue.[76] While the Supreme Court of India has recognised a general right to privacy, no general right relating to personal data protection has been developed to date. On evidence, the specific issue of enforcement, therefore, remains a problem. The absence of a general data protection legislation and the political philosophy of non-regulatory policies have translated into self-regulation and implementation of industry codes.[77] But surprisingly it has also forced India to deploy a more proactive approach that seeks to find legal solutions for data protection and data privacy in order to protect the economic interests of the country. This perspective acknowledges that in a globalised world, the preservation of the value of privacy is also closely linked with the economic development of the country.[78] From this perspective, informational privacy requires some degree of social and legal control.

The subject matter of data protection in India has been dealt with by the Information Technology Act, 2000, No. 21 of 2000, but not in an exclusive manner.[79] One can argue that the legislation

---

*Union of India*, A.I.R. 1978 S.C. 597 (India), it was held that it would not be enough to say that a violation of privacy would be justified by law, it must further be shown that the law under which the violation has taken place is just, fair and reasonable.

[76] The debate concerning data protection and data privacy in India started due to offshore outsourcing wherein personal data was exported by overseas companies to their off-shore agents or counterparts in India. If it was not for this mushrooming off-shoring business, India would perhaps never have worried much about data protection, as there are already existing provisions in the Indian legal framework for the protection of data privacy.

[77] NASSCOM, the coordinating body for India's software services industry, has established the self-regulatory Data Security Council of India (DSCI) in order to establish, monitor and enforce privacy and data protection standards for India's information technology and outsourcing industry.

[78] *See* CHARLES D. RAAB ET AL., APPLICATION OF A METHODOLOGY DESIGNED TO ASSESS THE ADEQUACY OF THE LEVEL OF PROTECTION OF INDIVIDUALS WITH REGARD TO PROCESSING PERSONAL DATA: TEST OF THE METHOD ON SEVERAL CATEGORIES OF TRANSFER (1998).

[79] The Information Technology Act, 2000 provides for civil liability in case of data theft, computer database theft, and privacy violation. Section 43 of the Act covers instances such as: (a) computer trespass, violation of privacy, etc.; (b) unauthorised digital copying, downloading and extraction of data, computer database or information and theft of data held or stored in any media; (c) unauthorised transmission of data or programme residing within a computer,

seems to have largely neglected the issue of privacy of personally identifiable information. However, there are other statutes which provide some safeguards to the lack of explicit legislation.[80] The Recovery of Debts Due to Banks and Financial Institutions Act, 1993, No. 51 of 1993, codifies India's tradition of maintaining confidentiality in bank transactions. Privacy in telecommunications is regulated by the Telecom Regulatory Authority of India (TRAI). The Common Charter of Telecom Services for adoption by all Telecom Service providers stipulates that "all Service Providers assure that the privacy of their subscribers (not affecting the national security) shall be scrupulously guarded."[81] Additionally, according to the Credit Information Companies (Regulation) Act, 2005, No. 30 of 2005, credit information pertaining to individuals in India has to be collected as per privacy norms enunciated in the applicable regulations.[82] Certain older laws are also relevant. The Indian Contract Act, 1872, No. 9 of 1872, offers an alternative solution to protect data as Indian companies acting as 'data importers' may enter into contracts with 'data exporters' to adhere to a high standard of data protection. The Specific Relief Act, 1963, No. 47 of 1963, provides preventive relief in the form of temporary and perpetual injunctions in order to prevent the breach of an existent obligation, whether expressly or by implication. However, the outcomes, though, depend on judicial interpretation. The Indian Telegraph Act, 1885, No. 13 of 1885, recognises privacy as a right but the government has the power to intercept communication for national security.

Although the Information Technology Act, 2000 attempts to address the issue of protecting privacy rights, it fails to meet the breadth and depth of protection that the E.C. Directive mandates[83] as it only protects privacy rights from government action. It is unclear whether such protection extends to private actions. Furthermore, unlike the E.C. Directive which imposes liability on each participant within the chain of command of the data who failed to protect the sanctity of the data, existing Indian laws only prosecute those individuals who directly violate laws

---

computer system or computer network (cookies, spyware, GUID or digital profiling are not legally permissible); (d) data loss, data corruption, etc.; (e) computer data or computer database disruption, spamming, etc.; (f) denial of service attacks, data theft, fraud, forgery, etc.; (g) unauthorised access to computer data or computer databases; and (h) instances of data theft.

[80] A few of these laws are section 65, section 66 and section 72 of the Information Technology Act, 2000, No. 21 of 2000, the Indian Contract Act, 1872, No. 9 of 1872, section 406 and section 420 of the INDIA PEN. CODE, 1860, No. 45 of 1860, and the Indian Copyright Act, 1957, No. 14 of 1957.

[81] *See* TELECOM REGULATORY AUTHORITY OF INDIA – COMMON CHARTER OF TELECOM SERVICES (2005), *available at* http://www.trai.gov.in/citizencharter/comm_charter16mar2006.pdf.

[82] It is my understanding that companies collecting and storing the data have been made liable for suspected leak or alteration of this data.

[83] § 43(b) of the Information Technology Act, 2000 is limited in scope.

related to computer systems.[84] Companies or individuals are exempted from liability for breaches of data privacy unless such violations were made knowingly.[85] Moreover, unlike the E.C. Directive which protects against data breaches by limiting data collection and use, the Indian laws do not specify conditions under which data can be collected and used.[86]

The Information Technology Act, 2000 has introduced some form of control over the use of encryption for communication in India.[87] The viability of this provision, however, remains questionable although the right to an encrypted transmission may be viewed as integral to the right to privacy flowing from Article 21 of the Constitution. The right can only be curbed by a 'procedure established by law.' As discussed before it is now well settled that such a procedure must be right, just, fair and reasonable to be valid. Whether the procedure under section 69 is sufficient to thwart the right to privacy remains to be tested.

It had become increasingly evident that the Information Technology Act, 2000 did not have suitable privacy and data protection provisions, and so the Indian government had appointed an Expert Committee on Cyber Laws whose role was to suggest amendments. The Committee proposed the following: (i) a new section 43(2) relating to the handling of sensitive personal data or information with reasonable security practices and procedures thereto; (ii) gradation of severity of computer related offences under section 66, committed dishonestly or fraudulently and punishment thereof; (iii) fine-tuning of section 72(1); (iv) additional section 72(2) in relation to breach of confidentiality with intent to cause injury to a subscriber; (v) language of section 66 pertaining to computer related offences to be revised in order to be in line with section 43 related

[84] § 43(b) of the Information Technology Act, 2000 only provides desultory safeguards against breaches in data protection. The scope of section 43(b) is limited to the unauthorized downloading, copying or extraction of data from a computer system, essentially unauthorized access and theft of data from computer systems. Section 43(b) is limited in scope, and so fails to meet the breadth and depth of protection that the E.U. Directive mandates.

[85] § 79 of the Information Technology Act, 2000, No. 21 of 2000.

[86] The E.C. Directive mandates five principles in accordance with which data must be collected and processed, including the requirement that the collection of data must be specific to the purpose for which it is collected, and such purpose must be disclosed to the data subject. It is based on a set of data protection principles, which include the legitimate basis, purpose limitation, data quality, proportionality, and transparency principles, data security and confidentiality, data subjects' rights of access, rectification, deletion and objection, restrictions on onwards transfers, additional protection where special categories of data and direct marketing are involved, and a prohibition on automated individual decisions. The E.C. Directive also requires that data must be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. *See* Council Directive 1995/46, 1995 O.J. (L 281) 31 (EC).

[87] § 69 of the Information Technology Act, 2000, No. 21 of 2000. It provides the Controller of Certifying Authorities with the power to intercept any transmission if certain criteria are satisfied and one such criterion provided for is the security of the state and concerns about the sovereignty and integrity of the nation.

to the penalty for damage to computer resources.[88] The Information Technology Amendment Act, 2008, No. 10 of 2009[89] was enacted to set the ball rolling in addressing the lacuna of data protection laws in the country through Sections 43A[90] and 72A.

The Information Technology Act, 2000 (as amended) now requires companies to maintain reasonable security practices, and procedures as to sensitive personal data or information, but does not define the phrase 'reasonable security practices and procedures.' As understood from the section 43A, reasonable security practices and procedures are to be determined as per the following manner: "as defined between the parties by mutual agreement or as specified in any law for the time being in force or to be specified by the Central Government in consultation with such professional bodies or associations as it may deem fit."[91] However, till date there is no law specifying reasonable security practices and procedures, nor has the Central government defined the security practices and procedures to be implemented in order to protect vital data. In the absence of such defined security practices and procedures, it is open for the parties to enter into agreements and lay down their own methods to protect their sensitive information and section 43A not only provides the freedom for doing so but also penalises any breach of such contractual obligations.

---

[88] CRID – UNIVERSITY OF NAMUR, FIRST ANALYSIS OF THE PERSONAL DATA PROTECTION LAW IN INDIA (2005), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/final_report_india_en.pdf. The offences have been graded according to the degree of severity of the offence when committed by any person, dishonestly or fraudulently without the permission of the owner. Keeping in line with the broad principles in E.C. Directive 2000/31/EC, section 79 has been revised to bring out explicitly the extent of the liability of the intermediaries in certain cases.

[89] The Lok Sabha (the Lower House of the Parliament of India) had hurriedly passed the Information Technology (Amendment) Bill, 2008 without even a debate as the discussion centred on political one-upmanship, rather than legislation. It received the assent of the President of India on 5th February 2009 and it came into force on 27th October 2009.

[90] Section 43A reads as follows: Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected. Explanation: For the purposes of this section (i) body corporate means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities; (ii) reasonable security practices and procedures means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit; (iii) sensitive personal data or information means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

[91] § 43A of the Information Technology Act, 2000, No. 21 of 2000.

Policy discourses in India have emphasised external forces as drivers of privacy policies. Hence of more significance is the Personal Data Protection Bill, 2006[92] drafted for the protection of personal data and information of an individual collected for a specific purpose and to prevent its usage by other organisations for commercial or other purposes. The draft Bill states that the personal data of any person collected for "a particular purpose or; obtained in connection with any transaction, whether by appropriate Government or by any private organization, shall not be put to processing; without the consent of the person concerned."[93] This straightforward approach is to be commended; however it does get distracted from the diversity of culture to which this could be applied since, as noted earlier, the Indian conception of privacy, being rooted in the local culture, is rather different from the West. Even the E.U.'s Assessment of Adequacy Report acknowledged the effect of differing political and cultural values on the interpretations of standards of 'adequacy' of data privacy protection measures to meet the E.U. standards. A final difficulty is that of cultural and institutional non-equivalence. Hence, all judgments about adequate protection must remain sensitive to important cultural differences.

Over the years, conflicts over data protection standards have led to several major international efforts aimed at the harmonization of information privacy standards.[94] However, despite the growing convergence of international data protection policy, 'privacy' still means something very different in various cultural and national traditions, perhaps particularly in non-Western jurisdictions but by no means there alone.[95] There are more important issues especially in terms of making information users aware of the issues involved. Stringent norms of protection and security are unlikely to quickly transform the existing norms of privacy in the interplay of private and public realms in India. The benefits of homogeneity must be balanced with the rights of legitimate authorities to determine laws within their jurisdictions. Finally, the seminal issue that remains

---

[92] The Personal Data Protection Bill, 2006 which was presented in the Rajya Sabha (the Upper House of the Parliament of India) in 2006, is still to be passed. It is highly unlikely that it will be passed in next 12 months.

[93] The Personal Data Protection Bill, 2006 requires that every organisation, whether it be governmental or private, engaged in the commercial transaction and collection of the personal data of persons shall – report to the Data Controller the type of personal data and information being collected and the purpose for which it is being or proposed to be used; take adequate measures to maintain confidentiality and security in the handling of personal data and information; and collect only such information that is essential for completion of any transaction with the individual. In order to give effect to the provisions of this scheme, the Central government can make further provisions so long as they are not inconsistent with the existing provisions.

[94] *See* OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANS-BORDER FLOWS OF PERSONAL DATA (1980), *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

[95] *Supra* note 78, at 202.

even if the laws are in place is that it will still be required to be enforced in such manner as to provide any meaningful protection.

## VI

## CONCLUSION: INVENTING THE RIGHT WAY

The purpose of this paper has been to highlight the unjustified scaremongering of Western popular press which often portrays India in negative light when it comes to the protection of privacy. So should India think about reforming the law or could the issue be just about re-educating the people? Experience and evidence suggest that India should not take any deranged measures and should conduct an assessment of the necessity of the measure in question and its suitability for achieving its objective and the consequent balancing of the resulting restrictions. It should evaluate the options for general regulatory, legislative, self-regulatory and voluntary steps that can enhance privacy in order to ensure effectiveness. I would not deny that the creation of legal regulations are not always driven by practical needs; often it is driven by political aspirations and most of the time because of economic needs where dominant interest groups seek rules that allow markets to function more effectively. In my opinion, a key argument in favour of regulation is that it may be a more effective form of commitment than contractual arrangements. Gerety argues that the problem for the concept of privacy "comes not from the concept's meagreness but from its amplitude, for it has a protean capacity to be all things to all lawyers. A legal concept will do us little good if it expands like a gas to fill up the available space."[96] There can never be a purely legislative solution to privacy, neither there can be a 'model' legislative framework as socio-economic issues are unique to countries and have be considered in their own right for alleviating concerns over privacy. India could develop a new model, a model that is particularly Indian.

The independent existence of the right to privacy, as emerging from the customs and traditions of the people in addition to being a statutory right, must be recognised. I do not agree that 'umbrella' data privacy legislation similar to the E.U. Directive should ever be enacted by India, particularly when the E.U. Directive in itself is seen as a serious obstacle to global commerce and e-commerce. I also argue that it is also not the first time that different countries have responded differently to legal issues arising due to a technological development. Over the last decade or so, an increasing amount of studies point out how countries have varying routines in addressing public problems, in conducting public debates, in making public policies and in evaluating 'evidence' brought forward

[96] Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 234 (1977).

in the context of such problems.[97] Since inception, the E.U. Directive has been severely criticised. However, it is thriving because of the conceptual vacuum surrounding the legal notions of privacy. Bergkamp also questions the often presumed desirability and necessity of the E.U. Directive.[98] Although, the E.U. data protection regime was conceived as a linear, single-issue scheme, it became paradoxical and has had several unintended adverse effects. According to the E.U. Directive, the notion of personal data is very wide so as to cover all information which may be linked to an individual. However, there are no necessarily sufficient safeguards to ensure that data does not become personal data when it is not intended to be as such. The E.U. Directive represents one of the most restrictive data privacy laws in existence on the planet; it imposes an onerous set of requirements on any person who collects or processes data pertaining to individuals in their personal or professional capacity. It is argued that the restrictive approach of the E.U. towards data privacy laws is justified as it espouses the protection afforded by E.U. law. However, this approach is criticised by multinational organisations on the grounds that it creates an intolerable global trading environment and also because it hampers free trade. Indeed, it is remarkable that governments have been able to adopt and implement such an onerous, expensive and paradoxical data protection regime without any plausible evidence of harm or threatened harm, entirely based on some vague notion of a 'fundamental right' and hypothetical risks. In its rhetoric, the E.U. has misled the public to believe that its data protection regime was merely an implementation of pre-existing fundamental rights. Where law is an appropriate and effective instrument, there is a need to identify the harm with precision so that a precise and targeted solution is arrived at that does not cause 'collateral damage.' If we want to achieve global privacy standards, the E.U. will have to demonstrate greater respect for other countries' approaches to privacy regimes.

In a pluralistic society where democratic traditions require compromise and consensus, the obvious solution I strongly recommend is a balancing framework based on a realistic set of standards that weighs the benefits of the free flow of information against the possible threats to privacy on a case-by-case basis. My argument fits well with Dworkin's theory of law[99] which supports the balancing of interests when the quest is for a single right answer and also favours the utilitarian approach of relying upon the consequences of actions. As I have mentioned before in this paper, there are several examples of Indian companies acting as 'data importers' entering into

---

[97] *See* SHEILA JASANOFF, DESIGNS ON NATURE: SCIENCE AND DEMOCRACY IN EUROPE AND THE UNITED STATES (2005).

[98] Lucas Bergkamp, *The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy*, 18 COMPUTER L. & SECURITY REP. 31 (2002).

[99] *See* Ronald Dworkin, *Hard Cases*, 88 HARV. L. REV. 1057 (1975).

contracts with 'data exporters' and also adhering to a high standard of data protection. These contracts are binding and fulfil the requirements of the overseas customers' national legislations.[100] A large number of Indian companies that are active in the information technology and outsourcing sectors at present have very stringent policies in relation to the protection of their clients' information and all employees are contractually bound to protect confidential information which may be processed.[101] The employment contracts clearly specify that the employees have to maintain as secret and confidential all such information which the company specifies from time to time. Many service providers in India have also engaged in voluntary self-regulation and adopted stringent security measures to reduce the risk of misuse of non-public personal data. Further, the establishment of the Data Security Council of India (DSCI) under the auspices of NASSCOM is definitely a positive step in the right direction. The objective of the DSCI is to create trustworthiness amongst Indian companies as global service providers by generating awareness of privacy and security issues. This re-emphasises my initial argument of not having the need to enact separate data privacy legislation modelled after the E.U. Directive.

I propose that the concept of privacy be imagined as a part of the 'collective good' which is important for the furtherance of 'social good,' thus leaving it open to us to adopt a broader concept of privacy and to determine how extensively it ought to be protected. Ironically, this is conceptually quite different from the more 'individual' Western perception. It is absolutely imperative that these standards are aligned to today's commercial realities and political needs, but they must also reflect technological realities. The implications of this view are significant. Perhaps most basic is the assumed fact of human diversity, wherein, as Locke put it, "men may choose different things, and yet all choose right." The regulation of privacy cannot be focused just on legislation and in any event will soon prove too complex. The way forward would be to move from precarious and unwarranted data protection legislation to the creation of effective policies which are designed to change the public perception of privacy as it cannot be denied that those who possess or process private information should bear a duty of confidentiality with respect to its dissemination.

---

[100] For example, all of the contracts with US based companies contain terms and specific conditions in relation to data protection that are in line with the Gramm-Leach-Bliley Act of 1999 and the Health Insurance Portability and Accountability Act of 1996.

[101] NASSCOM has established the National Skills Registry (NSR), a database of verified employees that includes biometric details and allows employers to verify the staff that they are recruiting. The NSR currently has details in relation to around 100,000 employees.