CHAPTER - IV

LAW RELATING TO RIGHT OF PRIVACY
IN INDIA – AN ANALYSIS

4.0 Introduction

Human rights are those minimal rights individuals need to have against the state of other public authority by virtue of their being members of the human family, irrespective of any other consideration. The concept of human rights is founded on the ancient doctrine of natural rights based on natural is founded on the ancient doctrine of natural rights based on natural law. Ever since the beginning of civilized life in a political society, the shortcomings and tyranny and ruin powers have led people to seek higher laws. The concept of higher law binding human authorities was evolved and it came to be asserted that there were certain rights anterior to society. These were superior to rights created by human authorities, were universally applicable to have existed prior to the development political societies. These rights were mere ideologies and there was no agreed catalogue of them and no machinery for their enforcement until they were codified into national constitutions, as a judicially enforceable Bill of rights.¹

Ever since the United Nations General Assembly adopted the Universal Declaration on Human Rights in 1948 and declared “all human beings are born free and equal in dignity and rights and everyone is entitled to rights and freedoms without distinction of any kind……, the concern for human rights has assumed global dimension. It has been a subject of discussion in almost all national and International conferences, discourses deliberations, negotiations and transactions.

Awareness to protect human rights has grown to such an extent that today it is being used as a yardstick to measure the civilization of societies, states, regimes and positive laws. It is being used as criteria for making value judgments, both the individuals and Government. It is being used as limitations on the Governments and authorities. It is being used as vehicle of development in every International monetary and humanitarian aid.

Promotion and protection of human rights ensures prevalence of freedom justice, peace and order in each society. It ensures recognition of worth of individual on equal basis. It ensures that every human being fulfils a quality, life based equality, dignity, respect and concern.

Observation of human rights is very essential and vital for every society to live in peace harmony and brotherhood. Observance of human rights is a complex one, more so in this multi-cultural, multi-lingual society like ours. Yet it is possible through co-operations with each individual observes it in his relations with other individuals, groups and society. It is possible when each individual respects the life of other as his own and when each thinks the dignity of the others is as important as his own. For it's a human rights culture has to be developed in each component society.

Human rights are universal, inviolable and inherent in every human being. 'Privacy', as the most valuable human right of all, is protected in several important national, regional and international instruments. It has several dimensions, including but not limited to privacy of a person, personal communications, personal data and territorial privacy. The right to privacy which is the highly essential part of one's life and personal liberty plays a significant role in the development of one's personality, integrity and dignity. However, certain practices such as bugging, telephone tapping and interception pose threats to the confidentiality of communications.

### 4.1 Development of Privacy Right in India - The Vedic Approach to Rights

If we try to characterize the politico-socio-cultural spirit of last one and half century in one word, the most appropriate term will be 'rights'. 'Right' has become the most powerful idiom of our contemporary intellectual discourse and many of the influential political theories developed in last one and a half century have focused their attention primarily on this concept. The meaning, essence and the ultimate end of human existence is understood in terms of rights only, and man's relationship with society and his fellow human beings is defined primarily in reference to this notion. In fact, most of

---

the political, social, moral, legal, cultural and even religious institutions of our present day society use 'rights' as the key concept, not only to define but also to 'justify' their existence. And in my view, the root cause of the major problems confronting our contemporary world lies in this right-centric world-view.

This world-view perceives men as "Little Gods" having 'rights' as 'absolute powers' to be used as defence weapons in their war against fellow beings or society as a whole. As a result, individual ego has overpowered the community spirit and humanity has split into factions of races, classes, cultures, genders, groups, professions, religions and ideologies. The unity conferring principles of the whole humanity are lost and man has emerged as an isolated individual having no emotional bondage with the larger reality which we can call 'NATURE'. This has deprived man of the essential purpose and meaning of life.

A plausible solution to this situation can be developed by replacing this right-centric world-view by obligation or duty-centric world-view, a world-view which maintains that 'obligation' and not 'right' is the fundamental notion to understand human reality. One of the most systematically developed examples of such a view can be found in classical Indian tradition which bases itself on the notions of Rina, Yajna and Purushartha.\(^4\)

Unlike most of the traditional Human Right Theories which claim that man is born with certain 'natural', inalienable, universal rights which can be ascribed to him just because he is a human being, this view maintains that man is born with certain Rinas (debts) or obligations and qua man, it is his foremost Dharma (duty) that he discharges these obligations with utmost care and perfection. Unless one does so, one is not considered worthy of being called a human being. In other words, the very essence and meaning of human existence consists in fulfilment of certain obligations - paying off some basic debts he is born with. To do so he may need certain privileges or facilities. He must be provided with these facilities. But he can possess these 'rightfully', only if he uses them for discharging his obligations.

In short, the whole system is based on a correlation between *svabhava* (one’s nature), *svadharma* (one’s duties) and *svadhikara* (one’s rights). From one’s specific nature certain specific duties follow and these duties create certain rights. Obviously, due to the variability of *svabhava*, modalities of rights also vary, but this variability in the distribution of social, economic or political rights, does not hamper the progress of society. Nor it is against the democratic spirit. On the contrary, it enhances the growth and stability of democratic society by providing special opportunities to each person to develop according to his own nature.

As is obvious, rights in this scheme are of derivative character. They are derived from a more fundamental notion i.e. of duty or obligation. Of course there is a strict duty-right correlation, but it is very different in nature from the usual characterization of such correlation where one person’s rights are supposed to give rise to duties of another person and vice-versa. Here one person’s obligations make the person himself the bearer of certain rights. The argument is, since I am morally bound to discharge certain obligations I must have corresponding rights which are necessary to enable me to perform my duties. Obviously, rights in this world-view are perceived not as "ends in themselves" but as necessary means or instruments to discharge certain obligations. As mentioned earlier, according to this system from *svabhava* (one’s nature) follows *svadharma* (one's duties), and from *svadharma* follows *svadhikara* rights. In other words, a person’s nature (qualities and capabilities), determines his duties and duties determine what rights he or she may possess. Not only the origin, but the nature, content and the scope of rights also depends on the nature, content and scope of the corresponding duties.

An interesting implication of this right-duty correlation is that it presents an example of the reciprocal derivation of ‘ought’ from ‘is’ and ‘is’ from ‘ought’. From the nature of man follow his duties, that is, what he ought to do, but from this ‘ought to’ follow his rights, that is, what he is supposed to possess as part of his nature.\(^5\)

Another implication of this right-duty correlation is that the nature and status of different rights necessarily correspond to the nature and the mode of duties from which

\(^5\) http://veda.wikidot.com/article:human-rights-the-indian-perspective visited on 19th Jan 2013 at 223 pm
they are derived. The more fundamental and essential the duty is, the more fundamental and essential will be the corresponding right. In other words, the degrees of the inalienability, universality, absoluteness and un-conditionality of rights will be determined by the mode and degrees of the different characteristics of the obligations for which these rights are supposed to function as means. This kind of approach naturally leads towards hierarchical categorization of rights in which rights are placed in order of their relative fundamentality determined by the fundamentality of the obligation they are meant to fulfil. For example, in this system human rights will be given priority over the rights of a civic person or the rights of a working person because, in comparison to the latter two, they flow from the duties which are more closely related to the fundamental and essential aspect of human nature. Even amongst different human rights this hierarchical ordering will be operative. Some rights will be considered more 'basic' than the others because these 'others' simply serve as helping or supportive instruments to realize the goals of these 'more basic' rights. In this system, problems regarding the conflict of rights are also settled by referring to the relative or proportional ordering of the corresponding duties.6

In this duty-centric world-view, rights acquire a goal-oriented character. They are not cherished for their own sake. They are important, but their importance primarily lies in their instrumentality towards specific goals. This goal oriented view of rights helps in setting some objective limits on the process of generating new rights (which appear to crop-up like mushrooms these days and seem to have become “licenses for madness”). Every system of rights, if it wants to avoid charges of arbitrariness, must provide a generative principle which must explain why certain rights must necessarily be included in the list and why certain others must necessarily be excluded. Why, for instance, it must include rights to certain things such as life, freedom, property or equality, and must definitely exclude certain other rights, such as right to deceive people, right to slavery, right to discriminate on the basis of colour, right to massacre a whole race or right to burn alive all black-haired men.7 Each time a new right is claimed or is demanded, the basic

6 Ibid
7 Why, for instance, it must include rights to certain things such as life, freedom, property or equality, and must definitely exclude certain other rights, such as right to deceive people, right to slavery, right to
question to be answered is - what goal it aims at? What purpose will it serve, and how essential, moral and just that purpose is? Answer to this question will definitely restrict indiscriminate and arbitrary inclusion of rights. Moreover, in this system, rights cannot be perceived and exercised as absolute, unconditional privileges or absolute unaccountable powers. Rather they can only be viewed as 'authentic' powers having legitimacy only as long as they are used for just purposes, in a just manner.

Thus, the system of rights advanced here puts an effective check on the possibility of the inclusion of putative immoral rights and cannot be misused to permit the pursuit of prima facie immoral ends.

The goal oriented character of rights also succeeds in keeping a right balance between the authority of the society or the State and the autonomy of the individual – the most disturbing problem of our present day political-social phenomena. On one hand it puts regulative limits on the exercise of rights by individuals; on the other hand it extends the area of society's obligations towards its members. It obliges society not only to remove hindrances in the path of the exercise of rights but also to provide structures and institutions which can create conditions appropriate for that exercise. Rights in this system do not remain confined to the mere guarantee of non interference from the external forces such as society or other human beings, but also become positive instruments in the realization of certain universal values.

Another important feature of this obligation based system is that it maintains that the roots of human rights lie in the spiritual aspect of human nature. Man as material individual is not only conditioned by the limitations of the physical world but can also be subjected to the coercion of society and its institutions. It is only his- temporal, spiritual destiny as a atman or soul (in the form of moksha) that makes him capable of transcending the limitations of time and space, history and culture, nation and state, race
and sex and provides him with some primordial rights as universal, unconditional and inalienable as the ultimate purushartha of moksha is.

It may be noted that this duty-based characterization of rights in no way diminishes their importance. Rather, it seems to add new dimensions to it. The strict duty-right correlation makes rights very specific, concrete and consequently more effective in the practical realm. They no more remain simply abstract principles capable of being variously interpreted or misinterpreted. They become concrete instruments of realizing the ultimate aims of human essence. Moreover, their derivation from moral obligation gives them significance of a 'value' and in a way makes them elements of ideal realm. Thus we see that the instrumentality of rights neither negates nor undermines their importance. On the contrary, it strengthens their theoretical plausibility and enhances their practical efficiency.

4.2 Constitutional Protections of Privacy with Judicial Interpretations

In 1965, the Supreme Court of India heard and decided State of U.P. v. Kaushaliya and others, a case which involved the question of whether women who are engaged in prostitution can be forcibly removed from their residences and places of occupation, or whether they were entitled, along with other citizens of India, to the fundamental right to move freely throughout the territory of India, and to reside and settle in any part of the territory of India under Article 19(1)(d) and (e) of the Constitution of India. In other words, did these women possess an absolute right of privacy over their decisions in respect to their occupation and place of residence? In its decision, the Supreme Court denied them this right holding that “the activities of a prostitute in a particular area... are so subversive of public morals and so destructive of public health that it is necessary in public interest to deport her from that place.” In view of their 'subversiveness', the statutory restrictions imposed by the Suppression of Immoral Traffic Act on prostitutes, were upheld by the court as constitutionally-permissible “reasonable restrictions” on their movements.

8 AIR 1964 SC 416
The legal alibis that the State employs to justify its infringement of our privacy are numerous, and range from ‘public interest’ to ‘security of the state’ to the “maintenance of law and order”. In this chapter the research investigator attempts to build a catalogue of these various justifications, without attempting to be exhaustive, with the objective of arriving at a rough taxonomy of such frequently invoked terms. In addition the research investigator also examines some of the more important justifications such as “public interest” and “security of the state” that have been invoked in statutes and upheld by courts to deprive persons of their privacy.

The statutory venues of deprivation of privacy by the state being many – strictly, any statute that imposes any restriction on movement, or authorizes the search or examination of any residence or book, or the interception of communication may be read as a violation of a privacy right — tracking each of these down would not only be an impossible exercise, but also contribute little to the analytical exercise we are attempting here. Instead, in this chapter we only list provisions from a few statutes that are the familiar instruments by which the state impinges on our privacy. This is done with the limited object of arriving at a rough inventory of the common technologies which the state employs to impinge on our privacy. Even if intrusions into our privacy are statutorily authorised, these statutes must withstand constitutional scrutiny.

Although not specifically referenced in the Constitution, the Right to Privacy is considered a ‘penumbral right’ under the Constitution i.e. a right that has been declared by the Supreme Court as integral to the Fundamental Right to Life and Liberty. In addition, although no single statute confers a cross-cutting ‘horizontal’ right to privacy various statutes contain provisions which either implicitly or explicitly preserve this right. The following sections provide an overview of both constitutional and statutory safeguards to privacy in India.

Although the Indian Constitution does not contain an explicit reference to a Right to Privacy, this right has been read in to the constitution by the Supreme Court as a component of two Fundamental Rights: the right to freedom under Article 19 and the

9 Article 21 of the Indian Constitution
right to life and personal liberty under Article 21. It would be instructive to provide a brief background to each of these Articles before delving deeper into the privacy jurisprudence expounded by the courts under them.\(^\text{10}\)

Part III of the Constitution of India (Articles 12 through 35) is titled ‘Fundamental Rights’ and lists out several rights which are regarded as fundamental to all citizens of India (some fundamental rights, notably the right to life and liberty apply all persons in India, whether they are ‘citizens’ or not). Article 13 forbids the State from making “any law which takes away or abridges” the fundamental rights.

Article 19(1) (a) stipulates that “All citizens shall have the right to freedom of speech and expression”. However this is qualified by Article 19(2) which states that this will not “affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence”.

Thus the Freedom of Expression guaranteed by Article 19(1) (a) is not absolute, but a qualified right that is susceptible, under the Constitutional scheme, to being curtailed under specified conditions.\(^\text{11}\)

The other important Fundamental Right from the perspective of privacy jurisprudence is Article 21 which reads “21. No person shall be deprived of his life or personal liberty except according to procedure established by law.” Where Article 19 contains a detailed list of conditions under which Freedom of Expression may be curtailed, by contrast Article 21 is thinly-worded and only requires a “procedure established by law” as a pre-condition for the deprivation of life and liberty. However,

\(^\text{10}\) http://www.iamai.in/Upload/IStandard/White%20Paper%20on%20Privacy,%202007.pdf visited on 19th Jan 2013 at 2.29 pm

\(^\text{11}\) Even the fundamental right “to freedom of speech and expression” as enumerated in Article 19(1)(a) of the Constitution of India comes with reasonable restrictions imposed by the State relating to (i) defamation; (ii) contempt of court; (iii) decency or morality; (iv) security of the State; (v) friendly relations with foreign states; (vi) incitement to an offence; (vii) public order; (viii) maintenance of the sovereignty and integrity of India. Thus, the right to privacy is limited against defamation, decency or morality.
the Supreme Court has held in a celebrated case *Maneka Gandhi v. Union of India*\(^{12}\) that any procedure "which deals with the modalities of regulating, restricting or even rejection of a fundamental right falling within Article 21 has to be fair, not foolish, carefully designed to effectuate, not to subvert, the substantive right itself. Thus, understood, "procedure" must rule out anything arbitrary, freakish or bizarre."

Shortly after independence, in a case challenging the constitutionality of search and seizure provisions, the Supreme Court dealt a blow to the right to privacy in India, holding that "When-the Constitution makers have thought fit not to subject [search and seizures] to Constitutional limitations by recognition of a fundamental right to privacy, analogous to the American Fourth Amendment, we have no justification to import it, into a totally different fundamental right."\(^{13}\)

Notwithstanding this early setback, five decisions by the Supreme Court in the succeeding five decades have established the Right to Privacy in India as flowing from Article 19 and 21.

The first was a seven-Judge bench decision in *Kharak Singh v. The State of U.P.*\(^{14}\) decided in 1964. The question for consideration in this case was whether "surveillance" under Chapter XX of the U.P. Police Regulations constituted an infringement of any of the fundamental rights guaranteed by Part III of the Constitution. Regulation 236(b) which permitted surveillance by "domiciliary visits at night" was held to be violative of Article 21. The meanings of the word "life" and the expression "personal liberty" in Article 21 were elaborately considered by this court in *Kharak Singh's case*. Although the majority found that the Constitution contained no explicit guarantee of a "right to privacy", it read the right to personal liberty expansively to include a right to

\(^{12}\) (1978) 2 SCR 621  
\(^{13}\)M. P. Sharma v Satish Chandra, AIR 1954 SC 300 (1954), http://indiankanoon.org/doc/1306519/ (last visited Oct 9, 2011). The court regarded the element of judicial supervision inherent in search orders issued under the CrPC as being sufficient safeguard against constitutional violations. "When such judicial function is interposed between the individual and the officer's authority for search, no circumvention thereby of the fundamental right is to be assumed. We are not unaware that in the present set up of the Magistracy in this country, it is not infrequently that the exercise of this judicial function is liable to serious error, as is alleged in the present case. But the existence of scope for such occasional error is no ground to assume circumvention of the constitutional guarantee"  
\(^{14}\) (1964) 1 SCR 332
dignity. It held that "an unauthorised intrusion into a person's home and the disturbance caused to him thereby, is as it were the violation of a common law right of a man - an ultimate essential of ordered liberty, if not of the very concept of civilization".

In a minority judgment in this case, Justice SubbaRao held that "the right to personal liberty takes in not only a right to be free from restrictions placed on his movements, but also free from encroachments on his private life. It is true our Constitution does not expressly declare a right to privacy as a fundamental right but the said right is an essential ingredient of personal liberty. Every democratic country sanctifies domestic life; it is expected to give him rest, physical happiness, peace of mind and security. In the last resort, a person's house, where he lives with his family, is his "castle" "it is his rampart against encroachment on his personal liberty." This case, especially Justice SubbaRao's observations, paved the way for later elaborations on the right to privacy using Article 21.

In 1972, the Supreme Court decided one of its first cases on the constitutionality of wiretapping. In R. M. Malkani v. State of Maharashtra\(^\text{15}\) the petitioner's voice had been recorded in the course of a telephonic conversation where he was attempting blackmail. He asserted in his defence that his right to privacy under Article 21 had been violated. The Supreme Court declined his plea holding that "The telephonic conversation of an innocent citizen will be protected by Courts against wrongful or high handed' interference by tapping the conversation. The protection is not for the guilty citizen against the efforts of the police to vindicate the law and prevent corruption of public servants."\(^\text{16}\)

The third case in the series, Govind v. State of Madhya Pradesh\(^\text{17}\), decided by a three Judge Bench of the Supreme Court, is regarded as being a setback to the right to privacy jurisprudence. Here, the court was evaluating the constitutional validity of Regulations 855 and 856 of the Madhya Pradesh Police Regulations which provided for police surveillance of habitual offenders which including domiciliary visits and picketing

---

\(^{15}\) AIR 1973 SC 157; 1973 SCR (2) 417

\(^{16}\) Ibid

\(^{17}\) (1975) 2 SCC 148
of the suspects. The Supreme Court desisted from striking down these invasive provisions holding that, "It cannot be said that surveillance by domiciliary visit-, would always be an unreasonable restriction upon the right of privacy. It is only persons who are suspected to be habitual criminals and those who are determined to lead a criminal life that are subjected to surveillance."

The Court went on to make some observations on the right to privacy under the constitution:

"Too broad a definition of privacy will raise serious questions about the propriety of judicial reliance on a right that is not explicit in the Constitution. The right to privacy will, therefore, necessarily, have to go through a process of case by case development. Hence, assuming that the right to personal liberty. The right to move freely throughout India and the freedom of speech create an independent fundamental right of privacy as an emanation from them it could not he absolute. It must be subject to restriction on the basis of compelling public interest. But the law infringing it must satisfy the compelling state interest test. It could not be that under these freedoms the Constitution-makers intended to protect or protected mere personal sensitiveness".

This case is important since it marks the beginning of a trend in the higher judiciary to regard the right to privacy as “not being absolute”. From Govind on wards, ‘non-absoluteness’ becomes the defining feature and the destiny of this right.

This line of reasoning was continued in Malak Singh v. State of Punjab & Haryana,\textsuperscript{18} where the Supreme Court held that surveillance was lawful and did not violate the right to personal liberty of a citizen as long as there was no ‘illegal interference’ and it was "unobtrusive and within bounds".

Nearly fifteen years separate this case from the Supreme Court’s next major elaboration of the right to privacy in R. Rajagopal v. State of Tamil Nadu\textsuperscript{19}. Here the court was involved a balancing of the right of privacy of citizens against the right of the press to criticize and comment on acts and conduct of public officials. The case related to

\textsuperscript{18} AIR 1981 SC 760
\textsuperscript{19} (1994) 6 S.C.C. 632
the publication by a newspaper of the autobiography of Auto Shankar who had been convicted and sentenced to death for committing six murders. In the autobiography, he had commented on his contact and relations with various high-ranking police officials—disclosures which would have been extremely sensational. Sometime before the publication, he appears to have been induced to write a letter disclaiming his authorship of the autobiography. On this basis, the Inspector General of Prisons issued a letter forbidding the newspaper from publishing the autobiography claiming, inter alia, that the publication of the autobiography would violate the prisoner’s privacy. Curiously, neither Shankar himself, nor his family were made parties to this petition. The Court decided to presume, somewhat oddly, that he had “neither written his autobiography” nor had he authorised its publication. The court then proceeded on this assumption to enquire whether he had any privacy interests that would be breached by unauthorised publication of his life story. The right of privacy of citizens was dealt with by the Supreme Court in the following terms:-

1. The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a “right to be let alone”. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, childbearing and education among other matters. None can publish anything concerning the above matters without his consent – whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages. Position may, however, be different, if a person voluntarily thrusts himself into controversy or voluntarily invites or raises a controversy.

2. The rule aforesaid is subject to the exception, that any publication concerning the aforesaid aspects becomes unobjectionable if such publication is based upon public records including court records. This is for the reason that once a matter becomes a matter of public record, the right to privacy no longer subsists and it becomes a legitimate subject for comment by press and media among others. We are, however, of the opinion that in the interests of decency [Article 19(2)] an exception must be

---

20 In the autobiography, he had commented on his contact and relations with various high-ranking police officials—disclosures which would have been extremely sensational.
carved out to this rule, viz., and a female who is the victim of a sexual assault, kidnap, abduction or a like offence should not further be subjected to the indignity of her name and the incident being publicised in press/media.

On this reasoning, the court upheld that the newspaper's right to publish Shankar's autobiography, even without his consent or authorisation, to the extent that this story was able to be pieced together from public records. However, if they went beyond that, the court held, "they may be invading his right to privacy and will be liable for the consequences in accordance with law." Importantly, the court held that "the remedy of the affected public officials/public figures, if any, is after the publication." 21

The final case that makes up the 'privacy quintet' in India was the case of PUCL v. Union of India 22, a public interest litigation, in which the court was called upon to consider whether wiretapping was an unconstitutional infringement of a citizen's right to privacy. The case was filed in light of a report brought out by the Central Bureau of Investigation on the 'Tapping of politicians' phones' which disclosed several irregularities in the tapping of telephones. On the concept of the 'right to privacy' in India, the Court made the following observations:

The right privacy - by itself - has not been identified under the Constitution. As a concept it may be too broad and moralistic to define it judicially. Whether right to privacy can be claimed or has been infringed in a given case would depend on the facts of the said case."

However, the Court went on to hold that "the right to hold a telephone conversation in the privacy of one's' home or office without interference can certainly be claimed as right to privacy". This was because "conversations on the telephone are often of an intimate and confidential character. Telephone conversation is an important facet of a man's private life. Right to privacy would certainly include telephone-conversation in the privacy of one's home or office. Telephone-tapping would, thus, infract Article 21 of the Constitution of India unless it is permitted under the procedure established by law."

21 ibid
22 AIR 1997 SC 568
The court also read this right to privacy as deriving from Article 19. "When a person is talking on telephone, he is exercising his right to freedom of speech and expression." the court observed, and therefore "telephone-tapping unless it comes within the grounds of restrictions under Article 19(2) would infract Article 19(1)(a) of the Constitution."

This case made two important contributions to communications privacy jurisprudence in India – the first was its rejection of the contention that ‘prior judicial scrutiny’ should be mandated before any wiretapping could take place. Instead, the court accepted the contention that administrative safeguards would be sufficient. Secondly, the Court prescribed a list of procedural guidelines, the observance of which would save the wiretapping power from unconstitutionality. In 2007, these safeguards were formally incorporated into the Rules framed under the Telegraph Act.23

Thus, to conclude, it may be observed that the right to privacy in India is, at its foundations a limited right rather than an absolute one. This limited nature of the right provides a somewhat unstable assurance of privacy since it is frequently made to yield to a range of conflicting interests – rights of paternity, national security etc which happen to have a more pronounced standing in law.

In March 2002, the National Commission to Review the Working of the Constitution submitted its report and recommended amending the Constitution to include a slew of new rights including the Right to Privacy. The new Right to Privacy would be numbered Article 21-B and would read:

"21-B. (1) every person has a right to respect for his private and family life, his home and his correspondence 
(2) Nothing in clause (1) shall prevent the State from making any law imposing reasonable restrictions on the exercise of the right conferred by clause (1), in the interests of security of the State, public safety or for the prevention of disorder or

23 Rule 419A of the Telegraph Rules stipulates the authorities from whom permission must be obtained for tapping, the manner in which such permission is to be granted and the safeguards to be observed while tapping communication. The Rule stipulates that any order permitting tapping of communication would lapse (unless renewed) in two months. In no case would tapping be permissible beyond 180 days. The Rule further requires all records of tapping to be destroyed after a period of two months from the lapse of the period of interception.
crime, or for the protection of health or morals, or for the protection of the rights
and freedoms of others.\textsuperscript{24}

There has, so far been no move to amend the constitution to give effect to this recommendation.

4.3 Privacy of Communications

4.3.1 Communications laws

All laws dealing with mediums of inter-personal communication – post, telegraph and telephone and email – contain similarly worded provisions permitting interception underspecified conditions.

Thus, section 26 of the India Post Office Act 1898 confers powers of interception of postal articles for the 'public good'. According to this section, this power may be invoked "On the occurrence of any public emergency, or in the interest of the public safety or tranquillity". The section further clarifies that "a certificate from the State or Central Government" would be conclusive proof as to the existence of a public emergency or interest of public safety or tranquillity.

Similarly, section 5(2) of the Telegraph Act authorizes the interception of any message

a) on the occurrence of any public emergency, or in the interest of the public safety; and
b) if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence,

Thus, the events that trigger an action of interception are the occurrence of any 'public emergency' or in the interests of 'public safety'.

Most recently, section 69 of the Information Technology Act 2008 contains a more expanded power of interception which may be exercised "when they [the authorised officers] are satisfied that it is necessary or expedient" to do so in the interest of

a) sovereignty or integrity of India,
b) defence of India,
c) security of the State,
d) friendly relations with foreign States, or
e) public order, or
f) preventing incitement to the commission of any cognizable offence relating to above, or
g) for investigation of any offence,

From a plain reading of these sections, there appears to be a gradual loosening of standards from the Post Office Act to the latest Information Technology Act. The Post Office Act requires the existence of a ‘state of public emergency’ or a ‘threat to public safety and tranquillity’ as a precursor to the exercise of the power of interception. This requirement is continued in the Telegraph Act with the addition of a few more conditions, such as expediency in the interests of sovereignty, etc. Under the most recent IT Act, the requirement of a public emergency or a threat to public safety is dispensed with entirely – here, the government may intercept merely if it feels it ‘necessary or expedient’.

In *Hukam Chand ShyamLal v. Union of India and others*25, the Supreme Court was required to interpret the meaning of ‘public emergency’. Here, the court was required to consider whether disconnection of a telephone could be ordered due to an ‘economic emergency’. The Government of Delhi had ordered the disconnection of the petitioner’s telephones due to their alleged involvement, through the use of telephones, in (then forbidden) forward trading in agricultural commodities. According to the government, this constituted an ‘economic emergency’ due to the escalating prices of food. Declining this contention, the Supreme Court held that:

---

a 'public emergency' within the contemplation of this section is one which raises problems concerning the interest of the public safety, the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or the prevention of incitement to the commission of an offence.

Economic emergency is not one of those matters expressly mentioned in the statute. Mere 'economic emergency'—as the high court calls it—may not necessarily amount to a 'public emergency' and justify action under this section unless it raises problems relating to the matters indicated in the section.

In addition the other qualifying term, 'public safety' was interpreted in an early case by the Supreme Court to mean "security of the public or their freedom from danger. In that sense, anything which tends to prevent dangers to public health may also be regarded as securing public safety. The meaning of the expression must, however, vary according to the context."

Thus, the words 'public emergency' and 'public safety' does provide some legal buffer before the government may impinge on our privacy in the case of post and telecommunications. In a sense, they operate both as limits on our privacy as well as limits on the government's ability to impinge on our privacy—since the government must demonstrate their existence to the satisfaction of the court, failing which their actions would be illegal.

However, as mentioned, even these requirements have been dispensed with in the case of electronic communications falling under the purview of the Information Technology Act where sweeping powers of interception have been provided extending from matters affecting the sovereignty of the nation, to the more mundane "investigation of any offence".

4.3.2 Privileged Communications

In addition to laying down procedural safeguards which restrict the conditions under which our communication may be intercepted, the law also safeguards our privacy.

---

in certain contexts by taking away the evidentiary value of certain communications. Thus, for instance, under the Evidence Act, communications between spouses and communications with legal advisors are accorded a special privilege.

Section 122 of the Evidence Act forbids married couples from disclosing any communications made between them during marriage without the consent of the person who made it. This however, does not apply in suits "between married persons, or proceedings in which one married person is prosecuted for any crime committed against the other."

This rule was applied in a case before the Kerala High Court, *T.J. Ponnenvs M.C. v. Varghese*27 where a man sued his son-in-law for defamation based on statements about him written in a letter addressed to his daughter. The trial court held that the prosecution was invalid since it was based on privileged communications between the couple. This was upheld by the high court. The petitioner had attempted to argue that it was immaterial how he gained possession of the letter. The high court disagreed with this contention holding that this would defeat the purpose of section 122.

Similarly section 126 forbids "barristers, attorneys, pleaders or vakils" from disclosing, without their client's express consent "any communication made to him in the course and for the purpose of his employment as such barrister, pleader, attorney or vakil... or to state the contents or condition of any document with which he has become acquainted in the course and for the purpose of his professional employment or to disclose any advice given by him to his client in the course and for the purpose of such employment."28

As with section 122, this privilege also comes with exceptions. Thus, the following kinds of communications are exempted from the privilege:

1. any communication made in furtherance of any illegal purpose,

---

27 *AIR 1967 Ker 228, 1967 Cri.L.J. 1511*
28 *Indian Evidence Act, 1872*
2. any fact observed by any barrister, pleader, attorney or vakil, in the course of his employment as such showing that any crime or fraud has been committed since the commencement of his employment.

Section 127 extends the scope attorney-client privilege to include any interpreters, clerks and servants of the attorney or barrister. They are also not permitted to disclose the contents of any communication between the attorney and her client.

Section 129 enacts a reciprocal protection and provides that clients shall not be compelled to disclose to the court any "confidential communication which has taken place between him and his legal professional adviser."

Section 131 of the Evidence Act further cements the legal protection afforded to married couples, attorneys and their clients by providing that "No one shall be compelled to produce documents in his possession, which any other person would be entitled to refuse to produce if they were in his possession" unless that person consents to the production of such documents.

These privileges do not limit the ability of the state to intercept communications—they merely negate the evidentiary value of any communications so intercepted.29


Under what circumstances may the State invade the privacy of our homes? What are the limits of these powers? Technically, any law that authorizes "search and seizure" can be said to authorize an invasion of our privacy. Many laws permit searches, for various grounds — ranging from the Income Tax Act which authorizes searches to recover undisclosed income, to the Narcotics Act which prescribes a procedure to search and seize drugs, to the Excise Act and the Customs Act which do so in order to discover goods that are manufactured or imported in violation of those respective statutes. In this section we deal only with the general provisions for search and seizure under the Code of Criminal Procedure.

The Code of Criminal Procedure (Cr.P.C) provides that a house or premises may be searched either under a search warrant issued by a court, or, in the absence of a court issued-warrant, by a police officer in the course of investigation of offences.

Thus, a court may issue a search warrant where

a) it has reason to believe that a person to whom a summons has been, or might be, addressed, will not or would not produce the document or thing as required by such summons; or
b) where such document or thing is not known to the court to be in the possession of any person, or
c) where the court considers that the purposes of any inquiry, trial or other proceeding under this Code will be served by a general search or inspection.

Similarly, section 165 of the Code of Criminal Procedure permits for searches to be conducted by “police officers in charge of police station or a police officer making an investigation” without first obtaining a warrant. Such a search may be conducted if he has “reasonable grounds for believing that anything necessary for the purposes of an investigation into any offence which he is authorised to investigate may be found in anyplace within the limits of the police station of which he is in charge, or to which he is attached”, and if, in his opinion, such thing cannot “be otherwise obtained without undue delay”.

Such officer must record in writing the grounds of his belief and specify “so far as possible” the thing for which search is to be made.

In both cases, the Code of Criminal Procedure requires the search to conform to procedures including the presence of “two or more independent and respectable inhabitants of the locality”. The preparation, in their presence, of “a list of all things seized in the course of such search, and of the places in which they are respectively found”, the delivery of this list to the occupant of the place being searched.

---

30 The Code of Criminal Procedure, 1973
31 Iyengar, Prashant, supra note 28.
However, in reality, these requirements are observed more in the breach. Courts have consistently held that not following these provisions would not make evidence obtained inadmissible — it would make the search irregular, not unlawful. Thus, in *State of Maharashtra v. Natwarlal Damodardas Soni* 32, where a search was conducted under the Customs Act to recover smuggled gold, the Supreme Court held that:

"Assuming that the search was illegal it would not affect either the validity of the seizure and further investigation by the customs authorities or the validity of the trial which followed on the complaint of the Assistant Collector of Customs".

In a different case, *Radhakrishan v. State of U.P.* 33 which involved an illegal search in contravention of the Code of Criminal Procedure, the Supreme Court held that:

"So far as the alleged illegality of the search is concerned, it is sufficient to say that even assuming that the search was illegal the seizure of the Articles is not vitiated. It may be that where the provisions of ... Code of Criminal Procedure, are contravened the search could be resisted by the person whose premises are sought to be searched. It may also be that because of the illegality of the search the Court may be inclined to examine carefully the evidence regarding the seizure. But beyond these two consequences no further consequence ensues".

India inherits the common law notion that "a man's house is his castle". In the light of the cases discussed above, this claim certainly appears to be lofty. However, there is still hope. In a recent case, the Supreme Court struck down provisions of a legislation on grounds that it was too intrusive of citizens' right to privacy. The case involved an evaluation of the Andhra Pradesh Stamp Act which authorized the collector to delegate "any person" to enter any premises in order to search for and impound any document that was found to be improperly stamped. Thus, for instance, banks could be compelled to cede all documents in their custody, including clients documents, for inspection on the mere chance that some of them may be improperly stamped. These banks were then

---

33 [1963] Supp. 1 S.C.R. 408
compelled under law to pay the deficit stamp duty on the documents, even if they themselves were not party to the transactions recorded in the documents.34

After an exhaustive analysis of privacy laws across the world, and in India, the Supreme Court held that in the absence of any safeguards as to probable or reasonable cause or reasonable basis, this provision was violative of the constitutionally guaranteed right to privacy “both of the house and of the person”.35

The case marks a welcome redrawing of the boundaries of the right to privacy against state intrusion.

4.5 Privacy of the Body

This section deals with the question of the extent of right to privacy with one’s own body in the context of four issues that have arisen before courts a) the ability of the state to order persons to undergo medical-examination, b) to undergo a range of “truth technologies” including narco analysis, brain mapping, etc., c) to submit to DNA testing and d) to abortion. In most cases, as we shall see, the right to privacy cedes ground to any available competing interest.

4.5.1 Court-ordered Medical Examinations

Can courts compel persons to undergo medical examinations against their will? In the case of Sharda v. Dharmapat36, the Supreme Court held that they could. Here a man filed for divorce on that grounds that his wife suffered from a mental illness. In order to establish his case, he requested the court to direct his wife to submit herself to a medical examination. The trial court and the high court both granted his application. On appeal to the Supreme Court, the woman contested the order on grounds firstly, that compelling a person to undergo a medical examination by an order of the court would be violative of her right to ‘personal liberty’ guaranteed under Article 21 of the Constitution of India. Secondly, in absence of a specific empowering provision, a court dealing with

34Iyengar, Prashant, supra note 28.
35Distt .Registrar & Collector, Hyderabad v. Canara Bank etc. AIR 2005 SC 186
362003] 4 SCC 493
matrimonial cases cannot subject a party to undergo medical examination against his her volition. The court could merely draw an adverse inference.

The Supreme Court rejected these contentions holding that the right to privacy in India was not absolute. If the "respondent avoids such medical examination on the ground that it violates his/her right to privacy or for a matter right to personal liberty as enshrined under Article 21 of the Constitution of India, then it may in most of such cases become impossible to arrive at a conclusion. It may render the very grounds on which divorce is permissible nugatory."

The Court upheld the rights of matrimonial courts to order a person to undergo medical test. Such an order, the court held, would not be in violation of the right to personal liberty under Article 21 of the Constitution of India. However, this power could only be exercised if the applicant had a strong prima facie case, and there was sufficient material before the court. Crucially, the court held that if, despite the order of the court, the respondent refused to submit herself to medical examination, the court would be entitled to draw an adverse inference against him.

Thus, oddly, one limitation on the right to privacy appears to be the statutory rights of others. One is entitled to the privacy of one’s body, to the extent that another person is not, thereby, deprived of a statutory right – as in this case, to divorce.

4.5.2 Reproductive Rights

To what extent do pregnant women enjoy a right to privacy over their bodies and their reproductive decisions? Are there circumstances when the State can intervene and either order or forbid an abortion?

According to the Medical Termination of Pregnancy Act, 1971 a pregnancy may be terminated before the twentieth week if:

(i) the continuance of the pregnancy would involve a risk to the life of the pregnant woman or of grave injury to her physical or mental health; or

(ii) there is a substantial risk that if the child were born, it would suffer from such physical or mental abnormalities to be seriously handicapped.
(iii) where any pregnancy is alleged by the pregnant woman to have been caused by rape,
(iv) where any pregnancy occurs as a result of failure of any device or method used by any married woman or her husband for the purpose of limiting the number of children,

Consent for termination needs to be obtained from the guardian in cases of minors or women who are mentally ill. In all other cases, the woman herself must consent.

Beyond the period of 20 weeks, the pregnancy may only be terminated if there is immediate danger to the life of the woman.

In August 2009, the Supreme Court heard an expedited appeal that was filed on behalf of a destitute mentally retarded woman who had become pregnant consequent to having been raped at a government run shelter. The government had approached the high court seeking permission to terminate her pregnancy, which had been granted by that court despite the finding by an ‘expert body’ of medical practitioners that she was keen on continuing the pregnancy. On appeal the Supreme Court held, very curiously, that the woman was not ‘mentally ill’, but ‘mentally retarded’, and consequently her consent was imperative under the Act.37 However, not content to stop there, the court made several puzzling and contradictory observations:

Firstly, the court took the opportunity to affirm, generally, women’s rights to make reproductive choices as a dimension of their ‘personal liberty’ as guaranteed by Article 21 (Right to Life and Personal Liberty) of the Constitution of India. The court observed:

“It is important to recognise that reproductive choices can be exercised to procreate as well as to abstain from procreating. The crucial consideration is that a woman’s right to privacy, dignity and bodily integrity should be respected. This means that there should be no restriction whatsoever on the exercise of reproductive choices such as a woman’s right to refuse participation in sexual

---

activity or alternatively the insistence on use of contraceptive methods. Furthermore, women are also free to choose birth-control methods such as undergoing sterilisation procedures. Taken to their logical conclusion, reproductive rights include a woman's entitlement to carry a pregnancy to its full term, to give birth and to subsequently raise children.\textsuperscript{38}

However, the court went on to affirm, in language that curiously imitates \textit{Roe v Wade}\textsuperscript{39}, that there was "a 'compelling state interest' in protecting the life of the prospective child."\textsuperscript{40}

Secondly, the Supreme Court upheld the woman's consent as determinative and in doing so, categorically rejected the high court approach. The court held that since she suffered from 'mild mental retardation' this did not render her "incapable of making decisions for herself". Simultaneously, however, the Supreme Court proceeded gratuitously to apply the common law doctrine of 'parenspatriae' to resume jurisdiction over the woman in her "best interests". According to a court-appointed expert committee, her mental age was "close to that of a nine-year old child" and she was capable of "learning through rote memorisation and imitation" and of performing "basic bodily functions". In this light, the court deemed in her 'best interests', as defined by an expert committee, to defer to her wishes.

The findings recorded by the expert body indicate that her mental age is closest that of a nine-year old child and that she is capable of learning through rote-memorisation and imitation. Even the preliminary medical opinion indicated that she had learnt to perform basic bodily functions and was capable of simple communications. In light of these findings, it is the 'best interests' test alone which should govern the inquiry in the present case and not the 'substituted judgment' test.\textsuperscript{41}

If one disregards the liberalism of its outcome, there are various problems with this decision. Chiefly, the Supreme Court relied on the woman's expressed consent to

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{38}Iyengar, Prashant, \textit{supra note} 28, p 18
\item \textsuperscript{39}410 U.S. 113 (1973)
\item \textsuperscript{40}Article 21 does not limit the abridgement of the right to life by the state to only cases where the state has compelling state interest. The Article reads "No person shall be deprived of his life or personal liberty except according to procedure established by law."
\item \textsuperscript{41}Iyengar, Prashant, \textit{supra note} 28, p. 19
\end{itemize}
\end{footnotesize}
deny the legitimacy of the high court’s decision in favour of abortion. Inexplicably, however, in the same move, the Supreme Court reserved to itself the right to adjudicate the ‘best interests’ of the woman. Thus, in relation to abortion, mentally retarded women are more autonomous than minor girls (since their own consent is determinative, rather than their guardians) but they are still less autonomous than ‘normal’ women (since their decisions are subject to adjudication based on what the court thinks is in their best interests)\textsuperscript{42}

4.5.3 DNA Tests in Civil Suits

Do we have a right to privacy over the interiors of our body – our blood, our tissue, our DNA? There is, by now, a strong line of cases decided by the Supreme Court in which our right to ‘bodily integrity’ has been held to not be absolute, and may be interfered with in order to settle many terrestrial issues. In most cases, this question has arisen in the context of the determination of paternity – either in divorce or maintenance proceedings. Central in the determination of these issues is section 112 of the Evidence Act which stipulates that birth of a child during the continuance of a valid marriage (or within 280 days of its dissolution) would be conclusive proof of legitimacy of that child, “unless it can be shown that the parties to the marriage had no access to each other at any time when he could have been begotten.”

As is evident, this section creates a strong legal presumption of legitimacy that leaves no room for a scientific rebuttal. Various litigants have, nevertheless, sought the courts ‘indulgence in accepting medical evidence to displace this formidable legal presumption. These efforts have yielded a measure of success, and a steady line of precedents since the early 1990s now affirms the right of courts to direct medical evidence in cases they consider fit. In these cases, the court has frequently invoked privacy rights as an important consideration to be weighed before ordering a person to submit to any test.

\textsuperscript{42}Iyengar, Prashant, supra note 28, p. 19
In one of the earliest and most frequently invoked cases, *Goutam Kundu vs State of West Bengal and Another* the Supreme Court laid down guidelines governing the power of courts to order blood tests. The court held:

1) "courts in India cannot order blood test as matter of course;
2) wherever applications are made for such prayers in order to have roving inquiry, the prayer for blood test cannot be entertained.
3) There must be a strong prima facie case in that the husband must establish on-access in order to dispel the presumption arising under section 112 of the Evidence Act.
4) The court must carefully examine as to what would be the consequence of ordering the blood test; whether it will have the effect of branding a child as a bastard and the mother as an unchaste woman.
5) No one can be compelled to give sample of blood for analysis."

On the particular facts of this case, the Supreme Court refused to order the respondent to submit to the test, since in its view, there was no prima facie case made out that cast doubts on the legal presumption of legitimacy.

These guidelines have been frequently invoked in subsequent cases. In a complex set of facts, in *Ms. X v. Mr. Z and Another* the Delhi High Court was called to consider whether a foetus had a 'right to privacy' – or whether the mother of the foetus could assert a right to privacy on its behalf. A woman had given birth to a still-born child and tissues from the foetus had been stored at the All India Institute of Medical Sciences. Her husband approached to obtain an order permitting a DNA test to be carried out to determine if he was the father. In her defence, the woman claimed that this would offend her right to privacy. The high court reaffirmed the guidelines laid down in the *Gautam Kundu case*, and also upheld the petitioner's right to privacy over her own body. However, the court took the stance that she did not have a right of privacy over the foetus once it had been discharged from her body:

---

45 Supra note 42
"The petitioner indeed has a right of privacy but is being not an absolute right, therefore, when a foetus has been preserved in All India Institute of Medical Science, the petitioner, who has already discharged the same cannot claim that it affects her right of privacy.

However, if the petitioner was being compelled to subject herself to blood test or otherwise, she indeed could raise a defence that she cannot be compelled to be a witness against herself in a criminal case or compelled to give evidence against her own even in a civil case but the position herein is different. The petitioner is not being compelled to do any such act. Something that she herself has discharged, probably with her consent, is claimed to be subjected to DNA test. In that view of the matter, in the peculiar facts, it cannot be termed that the petitioner has any right of privacy."

The decision has wide-ranging implications since it virtually divests control and ownership over any material that has been discarded from the body – from nails to hair to tissue samples. In an interesting case in the US, *Moore v. Regents of the University of California*46, the Supreme Court of California was faced with a suit to determine whether a man retained ownership over cells that had been removed from his body through a surgical procedure. In this case, cells from a patient’s spleen were used to conduct research which resulted in the patenting of a cell-line by the defendant. The patient sued for a share in the profits, but this was rejected by the court which held that he had no property rights to his discarded cells or any profits made from them. The court specifically rejected the argument that his spleen should be protected as property as an aspect of his privacy and dignity. The court held these interests were already protected by informed consent.

In a sense the *Ms. X v. Mr. Z case*47 arrives at identical conclusions without as much deliberation on its implications. It would be interesting to see how subsequent courts interpret and apply this precedent.

One of the most critical factors, consistently weighed by courts alongside the privacy rights implicated, is the ‘best interests’ of the child. Thus, in *Bhabani Prasad*

46 51 Cal. 3d 120; 271 Cal. Rptr. 146; 793 P.2d 479
47 *Supra note* 43
Jena v. Convenor Secretary, Orissa State Commission for Women & Anothers\textsuperscript{48}, the Supreme Court quashed a high court-mandated DNA test to determine the paternity of an unborn child in a woman's womb. In doing so, the Supreme Court observed:

"In a matter where paternity of a child is in issue before the court, the use of DNA is an extremely delicate and sensitive aspect. One view is that when modern science gives means of ascertaining the paternity of a child, there should not be any hesitation to use those means whenever the occasion requires. The other view is that the court must be reluctant in use of such scientific advances and tools which result in invasion of right to privacy of an individual and may not only be prejudicial to the rights of the parties but may have devastating effect on the child. Sometimes the result of such scientific test may bastardise an innocent child even though his mother and her spouse were living together during the time of conception. In our view, when there is apparent conflict between the right to privacy of a person not to submit himself forcibly to medical examination and duty of the court to reach the truth, the court must exercise its discretion only after balancing the interests of the parties and on due consideration whether, for a just decision in the matter, DNA is eminently needed."

A strong trend, evident in this case, is the bussing of the interests of the child (in not being declared illegitimate), along with the privacy rights of the mother. The two create a composite interest opposed to that of the putative father, which the courts have been reluctant to interfere with except for the most compelling reasons. But what happens when then the interests of the child conflict with the privacy rights of either parent?

In a high profile case in 2010, \textit{Shri Rohit Shekhar v. Shri Narayan Dutt Tiwari}\textsuperscript{49}, the Delhi High was called upon to determine whether a man had a right to subject the person he named as his biological father to a DNA test. Contrary to the trend in the preceding cases, it was the biological father who pleaded his right to privacy in this case. The court relied on international covenants to affirm the "right of the child to know of her (or his) biological antecedents" irrespective of her (or his) legitimacy. The court ruled:

\textsuperscript{48} AIR 2010 SC 2851 http://indiankanoon.org/doc/486945/ visited 25\textsuperscript{th} July 2013.  
There is of course the vital interest of child to not be branded illegitimate; yet the conclusiveness of the presumption created by the law in this regard must not act detriment to the interests of the child. If the interests of the child are best served by establishing paternity of someone who is not the husband of her (or his) mother, the court should not shut that consideration altogether. The protective cocoon of legitimacy, in such case, should not entomb the child’s aspiration to learn the truth of her or his paternity.

The court went on to draw a distinction between legitimacy and paternity that may both “be accorded recognition under Indian law without prejudice to each other. While legitimacy may be established by a legal presumption\(^50\), paternity has to be established by science and other reliable evidence”\(^51\) The court, however, reaffirmed that the same considerations would apply as was laid down in previous cases – i.e., the plaintiff would have to establish a prima facie case and weigh the competing interests of privacy and justice before it could order a DNA test. In this case, the petitioner was able to produce DNA evidence that excluded the possibility that his legal father was his biological father. In addition, photographic and testimonial evidence suggested that the respondent could be his biological father. On these grounds the Delhi High Court ordered the respondent to undergo a DNA test. This was upheld in an appeal to the Supreme Court.

So from the foregoing cases, it appears that it is the ‘best interests of the child’ that undergirds the right to privacy of either parent. When the two are in conflict it is the former that will, the case law suggests, invariably prevail.

4.5.4 Bodily Effects — Fingerprints, handwriting samples, photographs, Irises, Narco-analysis, brain maps and DNA

The human body easily betrays itself. We are incessantly dropping residues of our existence wherever we go – from shedding hair and fingernails, to fingerprints and footprints, handwriting – which, through use of modern technology, can implicate our bodies, and identify us against our will. Not even our thoughts are immune as new

\(^50\) Section 112 of the Indian Evidence Act, 1872
\(^51\) Supra note 48
technologies like brain mapping pretend to be able to harvest psychic clues from our physiology.

In this section we explore occasions when the state may compel us to 'perform' our existence for instance, by submitting to photography, providing finger impressions or handwriting samples, submit to narco-analysis and truth tests, and more recently to provide iris scan data or our DNA.

Section 73 of the Evidence Act stipulates that the court “may direct any person present in the court to write any words or figures for the purpose of enabling the court to compare the words or figures so written with any words or figures alleged to have been written by such person.”

This section was interpreted by the Supreme Court in *State of U.P. v. Ram Babu Misra* where it was held that there must be “some proceeding before the court in which...it might be necessary... to compare such writings”. This specifically excludes, say, a situation where the case is still under investigation and there is no present proceeding before the court. “The language of section 73 does not permit a court to give a direction to the accused to give specimen writings for anticipated necessity for comparison in a proceeding which may later be instituted in the court.”

The pre-independence *Identification of Prisoners Act*, 1920 provides for the mandatory taking, by police officers, of “measurements” and photograph of persons arrested or convicted for any offence punishable with rigorous imprisonment for a term of one year of upwards or ordered to give security for his good behaviour under section 118 of the Code of Criminal Procedure. The Act also empowers a magistrate to order a person to be measured or photographed if he is satisfied that it is required for the purposes of any investigation or proceeding under the Code of Criminal Procedure, 1898.54

---

53 Sections 3 & 4 of the *Identification of Prisoners Act*, 1920
54 *Ibid*, Section 5
The Act also provides for the destruction of all photographs and records of measurements on discharge or acquittal.\textsuperscript{55}

In addition, the Code of Criminal Procedure was amended in 2005 to enable the collection of a host of medical details from accused persons upon their arrest. Section 53 of the Code of Criminal Procedure provides that upon arrest, an accused person may be subjected to a medical examination if there are “reasonable grounds for believing” that such examination will afford evidence as to the crime. The scope of this examination was expanded in 2005 to include “the examination of blood, blood-stains, semen, swabs in case of sexual offences, sputum and sweat, hair samples and finger nail clippings by the use of modern and scientific techniques including DNA profiling and such other tests which the registered medical practitioner thinks necessary in a particular case.”

In a case in 2004, the Orissa High Court affirmed the legality of ordering a DNA test in criminal cases to ascertain the involvement of persons accused. Refusal to cooperate would result in an adverse inference drawn against the accused. After weighing the privacy concerns involved, the court laid down the following considerations as relevant before the DNA test could be ordered.

(i) “the extent to which the accused may have participated in the commission of the crime;

(ii) the gravity of the offence and the circumstances in which it is committed;

(iii) age, physical and mental health of the accused to the extent they are known;

(iv) whether there is less intrusive and practical way of collecting evidence tending to confirm or disprove the involvement of the accused in the crime;

(v) the reasons, if any, for the accused for refusing consent”\textsuperscript{56}

Most recently the draft DNA Profiling Bill pending before the Parliament attempts to create an ambitious centralized DNA bank that would store DNA records of virtually anyone who comes within any proximity to the criminal justice system. Specifically, records are maintained of suspects, offenders, missing persons and

\textsuperscript{55} Section 7

“volunteers”. The schedule to the Bill contains an expansive list of both civil and criminal cases where DNA data will be collected including cases of abortion, paternity suits and organ transplant. Provisions exist in the bill that limit access to and use of information contained in the records, and provide for their deletion on acquittal. These are welcome minimal guarantors of privacy.

It is evident that the utility of this mass of information – fingerprints, handwriting samples and photographs, DNA data – in solving crimes is immense. Without saying a word, it is possible for a person to be convicted based on these various bodily affects – the human body constantly bears witness and self-incriminates itself. Both handwriting and finger impressions beg the question of whether these would offend the protection against self-incrimination contained in Article 20(3) of our Constitution which provides that “No person accused of any offence shall be compelled to be a witness against himself.” This argument was considered by the Supreme Court in The State of Bombay v. Kathi Kahu Oghad and others. The petitioner contended that the obtaining of evidence through legislations such as the Identification of Prisoners Act amounted to compelling the person accused of an offence "to be a witness against himself" in contravention of Article 20(3) of the Constitution. The court held that “there was no infringement of Article 20(3) of the Constitution in compelling an accused person to give his specimen handwriting or signature, or impressions of his thumb, fingers, palm or foot to the investigating officer or under orders of a court for the purposes of comparison....Compulsion was not inherent in the receipt of information from an accused person in the custody of a police officer; it will be a question of fact in each case to be determined by the court on the evidence before it whether compulsion had been used in obtaining the information”.

Over the past two decades, forensics has shifted from trying to track down a criminal by following the trail left by her bodily traces, to attempting to apply a host of invasive technologies upon suspects in an attempt to escape truth and lies directly from their body. One statement by Dr M.S. Rao, Chief Forensic Scientist, Government of India captures this shift:

58 Ibid
Forensic psychology plays a vital role in detecting terrorist cases. Narco-analysis and brainwave fingerprinting can reveal future plans of terrorists and can be deciphered to prevent terror activities. Preventive forensics will play a key role in countering terror acts. Forensic potentials must be harnessed to detect and nullify their plans. Traditional methods have proved to be a failure to handle them. Forensic facilities should be brought to the doorstep of the common man. Forensic activism is the solution for better crime management.59

Although there are several such ‘technologies’ which operate on principles ranging from changes in respiration, to mapping the electrical activity in different areas of the brain, what is common to them all, in Lawrence Liang’s words is that they “maintain that there is a connection between body and mind; that physiological changes are indicative of mental states and emotions; and that information about an individual’s subjectivity and identity can be derived from these physiological and physiological measures of deception”60

So, how legal are these technologies, in view of the constitutional protections against self-incrimination? In a case in 2004 the Bombay High Court upheld these technologies by applying the logic of the Kathi Kalu Oghad case discussed above. The court drew a distinction between ‘statements’ and ‘testimonies’ and held that what was prohibited under Article 20(3) were only ‘statements’ that were made under compulsion by an accused. In the court’s opinion, “the tests of Brain Mapping and Lie Detector, in which the map of the brain is the result, or polygraph, then either cannot be said to be a statement”. At the most, the court held, “it can be called the information received or taken out from the witness.”61


60Ibid

This position was however overturned recently by the Supreme Court in Selvi v. State of Karnataka. In contrast with the Bombay High Court, the Supreme Court expressly invoked the right of privacy to hold these technologies unconstitutional.

"Even though these are non-invasive techniques the concern is not so much with the manner in which they are conducted but the consequences for the individuals who undergo the same. The use of techniques such as 'Brain Fingerprinting' and 'FMRI-based Lie-Detection' raise numerous concerns such as those of protecting mental privacy and the harms that may arise from inferences made about the subject's truthfulness or familiarity with the facts of a crime."

Further down, the court held that such techniques invaded the accused's mental privacy which was an integral aspect of their personal liberty.

"There are several ways in which the involuntary administration of either of the impugned tests could be viewed as a restraint on 'personal liberty' ... the drug induced revelations or the substantive inferences drawn from the measurement of the subject's physiological responses can be described as an intrusion into the subject's mental privacy"

Following a thorough-going examination of the issue, the Supreme Court directed that "no individual should be forcibly subjected to any of the techniques in question, whether in the context of investigation in criminal cases or otherwise. Doing so would amount to an unwarranted intrusion into personal liberty." The court however, left open the option of voluntary submission to such techniques and endorsed the following guidelines framed by the National Human Rights Commission

(i) No Lie Detector Tests should be administered except on the basis of consent of the accused. An option should be given to the accused whether he wishes to avail such test.

(ii) If the accused volunteers for a Lie Detector Test, he should be given access to a lawyer and the physical, emotional and legal implication of such a test should be explained to him by the police and his lawyer.

(iii) The consent should be recorded before a judicial magistrate.
(iv) During the hearing before the magistrate, the person alleged to have agreed should be duly represented by a lawyer.
(v) At the hearing, the person in question should also be told in clear terms that the statement that is made shall not be a 'confessional' statement to the magistrate but will have the status of a statement made to the police.
(vi) The magistrate shall consider all factors relating to the detention including the length of detention and the nature of the interrogation.
(vii) The actual recording of the lie detector test shall be done by an independent agency (such as a hospital) and conducted in the presence of a lawyer.
(viii) A full medical and factual narration of the manner of the information received must be taken on record.

Although the right against self-incrimination and the inherent fallaciousness of the technologies were the main ground on which decision ultimately rested, this case is valuable for the court's articulation of a right of 'mental privacy' grounded on the fundamental right to life and personal liberty. It remains to be seen whether this articulation will find resonance in other determinations in domains such as, say, communications.

4.6 Privacy of Records

Since at least the mid-nineteenth century, we have been living in what Nicholas Dirks has termed an "ethnographic state" – engaged relentlessly and fetishistically in the production and accumulation of facts about us. From records of birth and death, to our academic records, most of our important transactions, our income tax filings, our food entitlements and our citizenship, most of us have assuredly been documented and lead a shadow existence somewhere on the files. Not only does the government keep records about us, but a host of private service providers including banks, hospitals, insurance and telecommunications companies maintain volumes of records about us. In this section the research investigator looks at the privacy expectation of records both maintained by the government and the private sector.
Various statutes require records to be maintained of activities conducted under their authority and entire bureaucracies exist solely in service of these documents. Thus, for instance, the Registration Act requires various registers to be kept which record documents which have been registered under the Act. Once registered under this Act, all documents become public documents and State Rules typically contain provisions enabling the public to obtain copies of all documents for a fee. Similarly, a number of legislation – typically dealing with land records at the state level contains enabling provisions that allow the public to access them upon payment of a fee.

Where no provisions are provided within the statute itself that enable the public to obtain records, two recourses are still available.

Firstly, the Evidence Act enables courts to access records maintained by any government body. Secondly, private citizens may access records kept in public offices through the Right to Information Act. Each of these avenues is described in some details below:

Section 74 of the Evidence Act defines “public documents” as including the following:

1. Documents forming the acts, or records of the acts

   (i) Of the sovereign authority,

   (ii) Of Official bodies and the Tribunals, and

   (iii) Of public officers, legislative, judicial and executive, of any part of India or of the Commonwealth, or of a foreign country.

2. Public records kept in any state of private documents.

It is clear from this definition that most records maintained by any government body are regarded as public documents. Section 76 mandates that every public officer “having custody of a public document, which any person has a right to inspect, shall give that person on demand a copy of it on payment of the legal fees there for together with a

---

63 Section 52 of the Registration Act 1908
certificate written at the foot of such copy that it is a true copy of such document or part thereof’.

Since there is no legislative guidance within the Evidence Act to indicate who may be said to possess “a right to inspect”, this has been interpreted to mean that where the right to inspect and take a copy is not expressly conferred by a statute (as in the Registration Act mentioned above), “the extent of such right depends on the interest which the applicant has in what he wants to copy, and what is reasonably necessary for the protection of such interest”. So it isn’t any officious meddler who may access such records – only persons with genuine interests in the matter, either personal or pecuniary, may obtain copies through this route.

In addition to the Evidence Act, copies of documents may also be obtained under the Right to Information Act 2005 which confers on citizens the right to inspect and take copies of any information held by or under the control of any public authority. Information is defined widely to include “any material in any form, including records, documents, memos, e-mails, opinions, advices, press releases, circulars, orders, logbooks, contracts, reports, papers, samples, models, data material held in any electronic form and information relating to any private body which can be accessed by a public authority under any other law for the time being in force”.

Section 8 (j) of the Act exempts “disclosure of personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual” unless the relevant authority “is satisfied that the larger public interest justifies the disclosure of such information”.

In an interesting case Mr. Ansari Masud A.K v. Ministry of External Affairs, the Central Information Commission has held that “details of a passport are readily made available by any individual in a number of instances, example to travel agents, at airline counters, and whenever proof of residence for telephone connections etc. is required. For this reason, disclosure of details of a passport cannot be considered as causing

unwarranted invasion of the privacy of an individual and, therefore, is not exempted from disclosure under Section 8(1)(j) of the RTI Act.” This is despite the fact that nothing in the Passport Act itself authorizes disclosure of any documents under any circumstances. However, the Right to Information Act isn’t as convenient a vehicle for privacy abuse as this case may suggest. The RTI adjudicatory apparatus has on several occasions upheld the denial of information on grounds of privacy violation — most famously in a case where an applicant sought information from the Census Department on the ‘religion and faith’ of Sonia Gandhi — the President of the largest party currently in power in India. Both the Central Information Commission — the apex body adjudicating RTI appeals as well as the Punjab and Haryana High Court upheld the denial of information as it would otherwise lead to an unwarranted incursion into her privacy.65

A similar concept of ‘public interest’ would seem to apply when private companies disclose personal information without a person’s consent. Without delving into the issue in too much detail, it would suffice here to mention one of the most important cases to have come up on the issue. In Mr. X v. Hospital Z66, a person sued a hospital for having disclosed his HIV status to his fiancé without his knowledge resulting in their wedding being called off. The Supreme Court held that the hospital was not guilty of a violation of privacy since the disclosure was made to protect the public interest. While affirming the duty of confidentiality owed to patients, the court ruled that the right to privacy was not absolute and was “subject to such action as may be lawfully taken for the prevention of crime or disorder or protection of health or morals or protection of rights and freedom of others.”

4.7 The Grey areas of Right to Privacy

Considering that the international community regards the right to privacy and data protection as a basic human right, India may be under a moral as well as legal obligation to enact privacy and data protection regulations. There are two modes in which regulations can be adopted: Self-regulation and Government regulation.

a) Self-regulation- India could consider promoting an initiative among Indian industries, especially those interested in the growth of e-commerce. Self-regulation by the industry offers the advantage of a flexible policy made by those who know the trade practices and are motivated by the desire of customers. Self-regulation is also cost efficient to the government, as enforcement mechanisms need not be established. However, a large and heterogeneous group of agents may make self-regulation difficult. However, there is also the risk that self-regulatory solution would be to set the lowest standard.

b) Government Regulation- Alternatively, the Indian government could adopt specific legislation to address privacy and data protection issue. Even countries like the US that have primarily taken a self-regulatory approach to protecting privacy on the Internet, are slowly moving towards Government regulation to bring about uniformity and effective application of privacy standards.

4.7.1 Issues to be considered

Enumerated below are some of the issues that the Indian Legislature should try to keep in mind while drafting a privacy law.

Protection from arbitrary and unlawful interference: by the Government and private parties- The legislation must ensure that an individual’s right to privacy is not interfered with in an arbitrary and unlawful fashion. Presently, judicial precedents prohibit violation of the right to privacy of an individual by Government agencies. A comprehensive law must provide for protection from intrusion by the Government as well as private parties.

The law must also address issues relating to trespass upon individual privacy, audio and video surveillance and interception of communications (including digital and electronic communications).

It must also try and prohibit/curtail the use of cutting-edge technology to trespass upon privacy rights and personal data. Presently, the right to privacy on the Internet is
being threatened due to several elements such as web cookies, unsafe electronic payment systems, Internet service forms, browsers and spam mail.

Protection of medical records—Historically, medical records were used largely by physicians and medical insurers. However, with the creation of electronic records and large databases of medical information, the number of health care professionals and organizations with access to medical records has increased. While such availability allows for research that can improve the understanding of diseases and treatments across broad populations, the number of parties with routine access to personally identifiable

---

67 [http://www.cookiecentral.com/faq/](http://www.cookiecentral.com/faq/) (Last visited on 21st January 2013) A Cookie is a message given to a Web browser by a Web server. The browser stores the message in a text file called cookie.txt. The message is then sent back to the server each time the browser requests a page from the server. Cookies were initially designed to address the fact that Web sites didn't know whether a user is a first time or repeat visitor, and possibly prepare customized Web pages for them. The information placed in a cookie is not only useful in the context of e-commerce but cookies provide marketing information; they can track the ads that have been clicked on, in order to provide internet users with similar banner ads in the future. Cookies are a source of concern relating to privacy on the Internet, because of the ability to track the activities of users without their knowledge.

68 While purchasing anything on the Internet a consumer is required to use a credit card. This results in the transmission of a credit card number over the Internet, which is very sensitive personal data and the concern is that this information will then be re-used for another purpose or sold to direct marketers. Consumers are three to four times more likely to experience theft or misuse of their credit cards when they shop online. (Jupiter Media Metrix report on e-commerce fraud' by Jim Van Dyke) Part of the problem is that some web site owners don't understand how to secure their sites properly or how to hire skilled staff, or they lack the funding necessary to provide adequate security measures to ensure privacy protection.

69 While subscribing to most Internet services, or gaining membership to online clubs Web sites require visitors to provide some extremely personal information, without offering any assurance with regards to privacy of that information. To join, users are almost always required to give their name, address, telephone number, e-mail address, products bought etc. The primary purpose of gathering personal information about consumers is market research. The information collected helps online businesses to understand consumer trends and helps them target their consumers more effectively. This personal information is either used by the business collecting it or is often sold to other businesses with a view to getting direct access to the consumers they wish to target.

70 An Internet Browser interprets HTML the programming language of the Internet, into the words and graphics that are seen my Internet users when viewing a web page. It is a type of software that allows Internet users to navigate information databases. There have been many reports of security bugs in browsers, which can enable web sites to access your personal information while a person is surfing the web. Most manufactures of Internet browsers have attempted to fix the bugs to prevent access to sensitive personal data of the users of such browsers. However, the threat still persists and browsers could result in the leakage of information such as the e-mail address or username of the Internet user. To understand how browsers leak information to http servers refer to [http://www.cen.uiuc.edu/~ejk/WWW-privacy.html](http://www.cen.uiuc.edu/~ejk/WWW-privacy.html).

71 Spam is the use of e-mail addresses for a purpose that consumers have not consented for and constitute a violation of personal rights. Internet users who have purchased a product over the Internet or have their e-mail address published on a web site or have subscribed to a news service or who have participated in news groups or mailing lists, often receive unsolicited / spam e-mail. Some Internet Service Providers and other Internet businesses engage in the unlawful practice of selling lists of their customer's e-mail addresses to other companies. These companies use programs to generate bulk e-mail messages that are intended to advertise or promote a business, web site or product.
medical data has raised concern about the potential misuse of this data. It is essential that such data is not collected and sold to researchers in the field of biomedical science, without the consent of the patients. With the advent of the internet, it has become increasingly difficult to track such data and not only does it amount to an invasion of privacy, but it also amounts to breach of the duty of confidentiality that medical professionals owe their patients.

Protection of financial records – Financial records of individuals must also be protected from being distributed and circulated among banks and financial companies as it may also result in the misuse of such information.

Preventing excessive monitoring of employees by the employer – Another major concern, especially among the working class is the excessive surveillance of employees activities by their employers. Recently, Privacy Foundation, a non-profit group in the US, reported that about 100 million workers, or about 27 percent, are subject to continuous surveillance of their e-mail and Internet use. This is an issue of rising importance and must be dealt with in a comprehensive manner.

4.7.2 Principles that could be adopted

These principles are based on the Safe Harbour Principles adopted between EU and US.

a) Notice - The data subject must be given notice in clear language, when first asked for personal data, of the purpose of data collection, the identity of the data controller, the kinds of third parties with whom the data will be shared, how to contact the organization collecting or processing the data, and the choices available for limiting use or disclosure of the information.

b) Choice - The data subject must be given clear, affordable mechanisms by which he or she can opt out of having personal information used in any way that is inconsistent with the stated purposes of collection.

c) Onward transfer - Where the data controller has adhered to the principles of notice and choice, it may transfer personal data if it ascertains that the receiving party also complies with the safe harbour principles, or if it enters into a contractual agreement that the receiving party will guarantee at least the same level of data protection as the transmitting party. When disclosure is made to a third party that will perform under instructions of the data controller, it is not necessary to again provide notice or choice, but the onward transfer principle continues to apply.

d) Security - The data controller must take reasonable precautions to protect data from loss or misuse, and from unauthorized access, disclosure, alteration or destruction.

e) Data integrity - The data controller must take reasonable steps to ensure that data are accurate, complete and current.

f) Access - Data subjects must have reasonable access to their personal data and an opportunity to correct inaccurate information.

g) Enforcement - At minimum, enforcement mechanisms must include readily available and affordable recourse for the investigation of complaints and disputes, damages awarded where applicable, procedures for verifying the truthfulness of statements made by the data controller regarding its privacy practices, obligations of the data controller to remedy problems arising out of noncompliance, and sanctions sufficiently rigorous to ensure compliance.

Three employees of Mphasis, a Business Process Outsourcing ("BPO") firm, which runs call centre services for Citibank's U.S. customers in Bangalore, India were arrested for allegedly siphoning $350,000 from the accounts of Citibank's U.S. customers. These employees used their positions, which provided them access to Citibank customers, to induce four customers into giving out the personal identification numbers to their accounts, allowing the employees to illegally siphon funds out of those accounts.\footnote{While Mphasis maintained that its security procedures, especially detection and enforcement systems, were adequate, industry analysts warned that this incident could heavily impact the offshoring industry in India. Forrester Research, a U.S. publicly-traded independent technology and market research company}
The above mentioned illustration shows how ineffective the existent legal system in addition to being ill-equipped to protect the privacy of netizens, and also to tackle such cases.

The absence of appropriate statutory measures in India is becoming of greater concern to investors, corporations, the legislature, and the public in other nations. India is being urged to enact an adequate protection regime which dictates the appropriate parameters for the collection, storage and use of personal data by private and government entities. Given the international focus on India's data protection scheme, it is merely a matter of time before India enacts data protection laws. However, since intellectual property rights that lack enforcement are worthless, the seminal issue that remains once the data protection laws are in place is whether the laws will be enforced in such a manner as to provide any meaningful protection to data.

The existing enforcement that focuses on the business implications of technology change, stated that the breach would have "far-reaching" negative connotations for the offshore BPO industry and said that the high turnover of Indian call centre staff makes it increasingly difficult to adhere to security processes and sufficiently check backgrounds. A Forrester research note said: While the centre in Pune was BS 7799 [security certification] and CMM Levels [quality certification] certified, the breach still occurred. Clients and prospects should not be lulled into security complacency by the laundry list of certifications or process changes that suppliers roll out. Customers are going to have to implement their own aggressive requirements, such as eliminating writing instruments in their offshore centres and auditing bi-monthly to ensure that the vendor is following mandated processes. Andy McCue, Indian Call Centre Staff in $350.000 Citibank Theft, SILICON.COM, Apr. II, 2005, http://www.silicon.com/research/special reports/offshoringl O.3800003026.391 294 26.00. html (visited on 19th Jan 2013 at 2. 23 pm) Forrester also claimed offshore call centre growth could drop by as much as a third because of security concerns, regulatory pressure and a consumer backlash.


regime in India's legal system is pitifully deficient, marred by interminable delays in moving matters through the existing court system. India will be unable to provide adequate protection to data unless a solution is found to address the court delays, and procedures established for expediently prosecuting data protection breaches and compensating those harmed.

4.8 Emergence of the issue of Data Protection

The protection of data finds its roots in the individual's right to privacy doctrine. The right to privacy has been explicitly contained in or has inferentially been found to exist in the constitutions of most developed nations.

India does not currently have a specific data protection law. Data protection and privacy are given scattered and rather sparse coverage by existing laws. The existing data protection laws, discussed in some detail below, are strewn in laws pertaining to information technology, intellectual property, crimes, and contractual relations. Under increasing pressure from BPO operations and call centres in India that handle large volumes of data from the United States and Europe, the Indian government is contemplating the passage of a comprehensive law protecting data. Despite the urgency of the matter and pressure from internal and external fronts, India has delayed enactment of legislation for several years. The form of the legislation - whether umbrella, sectoral, or a combination of the two - which will provide optimal protection for cross-border data processed in India, has been under discussion for several years. At this point, it appears likely that India's Information Technology Act of 2000 ("IT Act of 2000") will be amended to incorporate laws that provide comprehensive protection to data. This

76 Peter Carey, Data Protection: A Practical Guide to UK And EU Law 23
78 Id.
79 An amendment to the IT Act of 2000, offering enhanced protection to data, was close to enactment in 2004, after 7 years in the making; unfortunately this proposed amendment was shelved due to a change of India's Central Government. McCue, Offshore Data, note 69.
approach, which continues to be discussed as the probable solution to India's data protection dilemma, does not entail enactment of a separate comprehensive law to deal with data security and privacy issues across all industries, as has been the case with the European Union.  

Until such time as India enacts adequate data protection laws, the current laws in India are the only protection offered for data privacy violations. These existing laws, including the IT Act of 2000 - which is the most pertinent since it pertains specifically to the use of computer data - have their shortcomings, which are discussed below. Unlike the Directive, which imposes liability on each participant within the chain of command who failed to protect the sanctity of the data, India's existing laws only prosecute those individuals who directly violate laws related to computer systems or copyright. Entities are exempt for breaches of data privacy, unless such a violation was made knowingly. Unlike the Directive, which protects data breaches by limiting its collection and use, the Indian laws do not specify conditions under which data can be collected and used.  

Where liability may be found by stretching the existing laws to cover breaches of data privacy, penalties afforded to victims are inadequate in a transnational context. The existing Indian laws and their deficiencies are addressed in further detail below.

4.8.1 Information Technology Act of 2000


81 Another alternative that was discussed, but is unlikely to be enacted, is an "umbrella" data privacy law similar to the E.U. Directive, which allows for sectoral adjustments. This proposal would encompass the E.U.'s comprehensive and expansive legislation, while retaining the flexibility of the U.S.'s sectoral approach. This proposal was offered by Rodney Ryder, a member of the committee considering data privacy/protection laws in India. E-mail from Rodney Ryder to Vinita Bali (Mar. 1, 2006) (on file with author).

82 The 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. See 23-27 and accompanying text. See generally infra note 80 and accompanying text.

83 IT Act of 2000, No. 21, §43(b).
Section 43(b) is limited in scope, and fails to meet the breadth and depth of protection that the E.U. Directive mandates. The law creates personal liability for illegal or unauthorized acts, while making little effort to ensure that internet service providers or network service providers, as well as entities handling data, be responsible for its safe distribution or processing. Furthermore, the liability of entities is diluted in Section 79 of the Act, which inserts "knowledge" and "best efforts" qualifiers prior to assessing penalties. A network service provider or intermediary is not liable for the breach of any third party data made available by him if he proves that the offence or contravention was committed without his knowledge, or that he had exercised all due diligence to prevent the commission of such offence or contravention. Similarly, while Section 85 of the Act does invoke entity liability, such liability is limited to the specified illegal acts under the IT Act of 2000, which does not offer broad protection of data. Section 85 does extend liability to key employees (managers, directors, officers, etc.) of the company for intentional or negligent acts that result in a breach of the specific violations under the IT Act of 2000.

With regard to damages available in the event of a breach of data privacy, Section 43(b) is deficient in that the maximum penalty for this breach is monetary compensation.

---

84 Ibid
85 Ibid, § 79
86 Ibid
87 Ibid, § 85 (emphasis added), which provides that:
(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there-under is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly: Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.
88 Ibid, §85(2) (emphasis added), which provides that: (2) Notwithstanding anything contained in subsection (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there-under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.
in the paltry amount of approximately $220,000.\(^9\) The maximum monetary damages available for a breach, which can potentially be worth several times more, are clearly inadequate in a transnational context. The law makes no differentiation based on the intentionality of the unauthorized breach, and no criminal penalties are associated with a breach of Section 43(b). The more limited crimes of computer hacking and tampering are considered criminal offenses under the IT Act of 2000: Section 65 offers protection against intentional or knowing destruction, alteration, or concealment of computer source code.\(^9\) Section 66, while offering no clear language that protects personal data, offers limited protection when personal data is destroyed, deleted or altered.\(^9\) Both Sections 65 and 66 are punishable with criminal penalties including jail time of up to 3 years or a monetary penalty of up to $440,000.\(^9\) Although Chapter XI of the IT Act of 2000 specifies criminal penalties for a laundry list of illegal acts, no such recourse is available for the broad realm of breaches of personal data security.\(^9\) In addition to the protections discussed above, Section 72 of the IT Act of 2000 offers some protection for breaches of confidentiality and privacy.\(^9\) Non-consensual disclosure of confidential information is punishable by imprisonment for up to 2 years, or a maximum fine of approximately $220,000.\(^9\)

\(^9\) IT Act of 2000, No. 21, §§ 43(b), 43(h)
\(^9\) Ibid. § 65
\(^9\) Ibid. § 66
\(^9\) Ibid. §§ 65, 66 Section 65 provides that:

> Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees [approximately $440,000], or with both.

Section 66(1) provides that: Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack. Section 66(2) provides for penalties similar to Section 65.

\(^9\) See generally ibid. ch. XI
\(^9\) Ibid. § 72. Section 72 provides that: Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

\(^9\) IT Act of 2000, No. 21 § 72
In contrast to the IT Act of 2000, the E.U. Directive envisions much broader violations associated with breach of data security than does the limited sphere of the IT Act of 2000. As described previously, the E.U. Directive provides for protections in the entire chain of control of data and creates systems of security and associated penalties within the various stages of data processing. For instance, the Directive prescribes limits to the collection of personal data, requiring that a purpose for the data collection be articulated. The 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; personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. 

The 1980 Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data promulgated by the Organization for Economic Cooperation and Development (the "OECD") are also instructive, demonstrating that a large void exists in India's IT Act of 2000. A reformation of the IT Act of 2000 should encompass the principles contained in the Directive, and the parallel OECD principles related to limitation of data collection, data quality, specified purpose, use limitation, security safeguards, individual participation and accountability.

Further, in matters of transnational data protection, the IT Act of 2000 is deficient in that jurisdiction for cases arising out of violations lies in India. A special tribunal is

---

97 Ibid
98 Ibid
99 Ibid
100 Organization for Economic Co-operation and Development ("OECD"), Information Security and Privacy, Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data, http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_00.html visited on 19th Jan 2013 at 2.23 pm
101 Principles of the Directive are discussed at notes 23-27 and accompanying text. See also Organization for Economic Cooperation and Development, Information Security and Privacy, Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data, http://www.oecd.org/document/18/0,2340, en_2649_34255_1815186_1_1_1_00.html visited Apr.16, 2007. The DECD Guidelines were formulated in anticipation that member nations, including the U.S., had agreed to pass legislation pertaining to data protection and privacy. The Guidelines were meant to address the threat that disparities in national legislations could hamper the free flow of personal data across national borders. It was anticipated that the flow of data would greatly increase with the innovation and spread of computer and communications technology. DECO, Information Security and Privacy, Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data, http://www.oecd.org/document/18/02340, en_2649_34255_1815186_1_1_1100.html. visited Apr.16, 2007).
established by the Central Government, and all matters arising out of the IT Act of 2000 are within the jurisdiction of this Cyber Appellate Tribunal.\textsuperscript{102} While the IT Act of 2000 is diligent in establishing a tribunal headed by a qualified judicial officer, the difficulty in accessibility to this tribunal is stark in a transnational setting.\textsuperscript{103} Injured parties who are non-residents of India would have to adjudicate disputes in a foreign jurisdiction, incurring the related expense and inconvenience thereof. The limited parties, from whom recourse and be sought, limited circumstances under which remedy may be established, and the limited nature of the damages is even barer when the avenues for recourse and compensatory sums are viewed from a perspective of third party nationals.

4.9 Alternatives to Current Enforcement Regimes in India

Once the data protection laws in India are strengthened, the general legal system must be tweaked in order to address data protection enforcement. Proposed remedies to fix the enforcement void include establishment of a national centralized enforcement body dedicated to, and trained in, electronic data piracy and enforcement. This national body must be given jurisdictional authority to enforce across state borders. In addition, it is essential to have specialized local police enforcement units which are specifically trained and maintained to recognize instances of, and enforce actions against, data piracy crimes. Finally, it is vital to adopt meaningful court reform to decrease burdens, costs and delays, and ensure that cases are concluded promptly with deterrent penalties and damages. Specialized judicial avenues of enforcement are the logical transition that India must make due to the in ability of the regular court system in India to deal with the additional volume of cases that cross-border crimes will generate. The solution is the establishment of specialized cyber infringement courts with jurisdiction overall violations related to intellectual property, including data privacy (hereinafter referred to as "Cyber Infringement Courts").\textsuperscript{104} The specific model for such a court depends on

\textsuperscript{102} IT Act of 2000, No. 21, §§ 48-64.
\textsuperscript{103} Ibid. §§ 46, 47
\textsuperscript{104} International tribunals dealing with cyber infringement are a second alternative. Given the cross-border nature of cyber breaches, and the ever increasing global interactions pertaining to intellectual property (including data privacy), these international tribunals may be an appropriate and effective solution in the future. In addition to the more commonly recognized areas of intellectual property (patents, trademarks, copyright, trade secret and unfair competition), data protection, database protection and privacy rights are areas related to, and encompassed within a broad definition of intellectual property. Cyber infringement
factors such as local customs and practices (including local procedural considerations), cyber infringement case loads, number of judges, and monetary considerations.105

4.9.1 Specialized Courts

Specialized courts are courts of limited and explicitly-focused subject matter jurisdiction. This jurisdictional feature means not only that the backlog in the regular courts gets reduced, but also that cases that fall within the jurisdiction of specialized courts get heard in an expedient, efficient manner. Another important feature of specialized courts is that, in contrast to judges of general jurisdiction courts who hear cases that span the entire spectrum of law, judicial officers who serve on specialized courts are typically experts in that field of law.106

Specialized courts can offer advantages related to time and efficiency in several ways. First, such courts foster judicial efficiency by virtue of the fact that in ceexperts are appointed to the bench in these courts, not much effort is expended in developing

courts may logically encompass all or a subset of these areas of intellectual property. See generally Int'l B. Ass'n., Intell. Prop. And Ent. Law Comm., International Survey of Specialised Intellectual Property Courts and Tribunals 6 (Sept. 2005) [hereinafter International Survey], available at www.commiba.orgattachmentarticles/88IFinal_International_IP_Survey_15-09-05.pdf. visited on 19th Jan 2013 at 2.23 pm) This model may draw from the Council of Europe's Convention on Cybercrime, an instrument for international cooperation which was signed on November 23,2001, by twenty-six Council of Europe Member States and the four non- Member States which had helped with the drafting (Canada, Japan, South Africa and the United States). The Convention requires parties to criminalize certain conduct that is committed through, against, or related to computer systems. Such substantive crimes include offenses against the confidentiality, integrity and availability of computer data and systems, as well as using computer systems to engage in conduct that would be criminal if committed outside the cyber-realm, i.e., forgery, fraud, child pornography, and certain copyright-related offenses. The Convention also requires parties to have the ability to investigate computer-related crime effectively and to obtain electronic evidence in all types of criminal investigations and proceedings. By providing for broad international cooperation in the form of extradition and mutual legal assistance, the Cybercrime Convention is intended to remove or minimize legal obstacles to international cooperation that delay or endanger a State's investigations and prosecutions of computer-related crime. See Press Release, Council of Europe, The Convention on Cybercrime, a Unique Instrument for International Co-operation (Nov. 23, 2001), available at www.hrea.org/lists/huridocs-techimarkup/msg00681.html. However, even at just a procedural level such international governance and enforcement would necessitate, among other things, that participating States: (1) enter into a treaty subjecting themselves to the jurisdiction of the international cyber crime tribunal, and (2) create a common set of rules or laws, including enforcement procedures, that would govern the area of intellectual property. Given the time consuming and costly nature of this solution, burdened with conceptual and procedural hurdles, this potential response is not a viable solution in the immediate future, 105 International Survey,

expertise to adjudicate the matters brought before them. This has the natural result of expediency in the processing of cases. The second advantage, a corollary to the first is that lawyers appearing in specialized courts expend less effort, and ultimately less client resources, in laying the foundational aspects of these complex areas of the law. In courts of general jurisdiction attorneys typically develop the legal framework by providing extensive background material through submissions to the court, in the form of written briefs, etc., to ensure that the judge has access to as much information as possible in order to adjudicate the case appropriately. Since judges in specialized courts are experts in the field and do not need this education, this directly results in focused submissions, as well as time and cost efficiency to the attorneys and their clients. A third advantage of specialized courts is the uniformity in decision making and consistency in the application of the law.

The expertise of the specialized court judge’s results in thoughtful, predictable and uniform rulings well grounded in the law, leading to certainty of decisions and containment of potential grounds for filing lawsuits. Therefore, courts are less likely to be burdened and overcrowded as fewer prospective litigants find grounds for bringing a dispute to court. A fourth related advantage is that given the soundness of the judgments of the court of initial jurisdiction (the specialized court), appeals are less likely to be filed. Therefore, the burden on appellate courts is also likely to be significantly reduced. Fifth, efficiency of time and procedure is also a likely result of the specialized nature of the proceedings. Judges who are experts in the field can better assess the time, procedure and substance required to move a case forward. Improved case management techniques, include establishing pre-trial deadlines, the discovery process, ruling on dispositive motions, moderating settlement proceedings, scheduling and conducting

---

107Ibid. (referring to generalist judges as "novices at everything and experts at nothing.").
108 Ibid
109 Ibid
110 Ibid
108 Ibid
111 Ibid
112 Ibid But (arguing that the uniformity of decisions and predictability in the case law can also be a cause for inefficiency. Counsel may determine that their chance of success in the specialized court is low due to the case law developed in these courts; a strategic decision may be made to posture the case in such a way that it falls within the jurisdiction of a general court. The effect of this is an unnecessary overburdening of the general court system, and an under-utilization of the specialized courts.)
113 Ibid.
112 Law Initiative
113 Ibid.
trials, etc. would result from the specialized judge who is familiar with the issues presented and would more effectively control the flow of litigation than a generalist judge. Finally, specialized courts can be used to support the generalized courts.

Due to the fluctuating and often erratic nature of court filings and proceedings, it is conceivable that a specialized court may have a small caseload at times. In such instances, specialized courts can lend a helping hand to overburdened courts of general jurisdiction. Due to the numerous advantages offered by specialized courts, these courts are a feature of the judicial systems of many countries, although their structure and function may vary. The first question to be addressed is the feasibility of specialized courts in India. If specialized courts are viable solutions to the Indian enforcement dilemma, then the next question is what model of specialized Cyber Infringement Courts would best fit India's needs with a view to proposing specific features of a specialized Cyber Infringement Court system with jurisdiction over civil and criminal intellectual property matters in India.

4.9.2 Specialized Courts a Feasible Solution to India's Problem of Enforcement of Data Protection

Specialized courts pose special problems for developing countries such as India. A major hurdle and in fact the greatest barrier, is the expense factor associated with the establishment of and maintenance of these courts. These costs are not only a one-time cost, but are also recurring in nature. The establishment expenses include consultation expenses related to policy research and drafting and design of new legislation; training of judicial officers, court and enforcement staff; administrative costs; and costs of acquiring and furnishing buildings to situate the specialized courts. Recurrent and on-going costs
must be reflected in larger budget allocation for agencies enforcing the legislation on-going training of court and administrative personnel, and hiring and retention of specialized judges, court and administrative agency staff.120

While the inherent expense of establishing specialized courts is significant, India is one of the developing nations that can afford, and indeed, must afford the support of its computer industry. India's gross domestic product grew 8.4% in 2005, topping $800 billion.121 It has grown at the second fastest rate in the world over the past three years, at an average of 8%.122 India's projected continued high economic growth, fuelled in large part by the growth in the computer-related industry, is the incentive for investing in a specialized court system that addresses breaches to the industry that is instrumental to India's incredible economic success. In other words, India cannot afford to "bite the hand that feeds it." If India is to meet economists' projections and develop in to one of the largest economies in the world within the next three decades, India "must expedite socio-economic reforms and take steps for overcoming institutional and infrastructure bottlenecks inherent in the system. The question, then, is not whether India can afford to establish specialized courts to address its enforcement problems. The appropriate question is whether India can afford to not invest in the security of its computer industry. If prompt enforcement is essential to deter crime, and if India's current judicial system is already over burdened, lethargic and inadequate, then the answer is clear. India must invest in a system of specialized courts to promptly and adequately adjudicate data privacy violations.

4.9.3 Proposed Features of India's Cyber Infringement Courts

While specific characteristics of the Cyber Infringements Courts are critical to their success in India, equally important is the public's ability to access justice through these courts. India's specialized Cyber Infringement Courts would ideally be located in strategic locations so as to provide reasonable access to litigants.

120 Ibid
122 10 Ways India
Given India's jurisdictional structure where there is one Supreme Court at the apex and a High Court in each State, at the very least one specialized court must be located in each State, and several others in each State strategically placed in proportion to the population density and anticipated flow of cyber infringement cases. Although the expense associated with the creation of such a network of specialized courts may appear prohibitive, India's economic outlook, and specifically the growth of the technology industry not only supports this judicial system, but indeed mandates it.

Data protection is an issue that is gaining increasing importance as our transnational exchange of private information grows. While the E. U. Has adopted stringent legislation to protect data, and the U.S. has reached agreement with the E.U. to offer protection, the Indian laws remain unsatisfactory. It is anticipated that India will soon enact legislation which will provide acceptable protection to private data. The issue that remains to be dealt with in the Indian context is, unfortunately, far larger than the enactment of strong protectionist laws. Laws act as a deterrent to wrongful conduct if they are applied with certainty and speed: both sadly deficient in the Indian judicial system. Unless addressed, the systemic problems of enforcement in India, and specifically, of unresolved cases due to court delays, will continue to render India's data protection laws inadequate.

---

123 India is a constitutional democracy, comprised of twenty-eight states, six Union Territories, and the Territory of Delhi (capital of India). It has a parliamentary system styled in the fashion of the British system. Its bicameral legislature consists of the upper house, or the Rajya Sabha, and the lower house, the Lok Sabha. Legislative power rests primarily with the Lok Sabha. The Prime Minister is the effective executive, though there is also a President who has limited powers. India's structure is explicitly federal, but with features that emphasize the power of the centre over sub-national units. The twenty-eight states, as well as Delhi and the Union Territory of Pondicherry have elected (unicameral) legislatures; the Chief Minister of each state is the chief executive. Each state also has a Governor, although appointed by the President, the Governor of each state works under the guidance and direction of the Prime Minister. Pawan Chaudhary 'Manmauji,' Indian Judicial System. Its Nature & Structure and Distinctions Between Law and Justice, in Indian Judicial System, Need and Directions of Reform, 25-27 (S.P. Verma ed. 2004) [hereinafter Indian Judicial System]

protection laws inadequate. Cyber Infringement Courts, specialized courts with jurisdiction over an intellectual property and data protection issues, are a necessary solution to India's enforcement problems. India must expediently adopt this system of specialized courts in order to render adequate protection to data and maintain its growing presence in the global technology arena.

4.10 Conclusion

Reflecting on the volume of case law in India on privacy, one is struck at once, both by the elasticity of the concept of privacy – spanning, as it does, diverse fields from criminal law to paternity suits to wiretapping – as well as its fragility – the flag of privacy is constantly being raised only to be ultimately overridden on pretexts that range from security of state, to a competing private interest.

On the one hand, one marvels at the success of the concept, only a few decades old in Indian law, in insinuating itself into legal arguments across diverse contexts. On the other hand, one is dismayed by the fact that rarely does the concept seem to score a victory. There is an almost ritual quality to the way in which the “right to privacy” is invoked in these cases - always named as a relevant factor; it never seems to substantially influence the outcome of the case at hand.

The right to privacy in India was an ‘Oops’ baby, born on the ventilator of a minority decision of the Supreme Court, and nourished in the decades that followed by sympathetic judges, who never failed to point out that this right was contingent – not absolute, not meant to be under the Constitution, but carved out anyway. Some five decades after its first invocation by the Supreme Court, one gets the feeling that the right to privacy, conceptually, hasn’t moved, and is still what it was then. We don’t, today, for the many times it has been invoked by courts, have a thicker, more robust concept of privacy than we started out with. So the question, that one is stuck with is, what work does this concept of privacy do?

One of the failings of the concept of privacy in India is that it doesn’t exist as a positive right, but is merely a resistive right against targeted intrusion. So for instance, the right to privacy would be useless as a concept to resist something like generalized
street video surveillance – as long as a citizen is not singled out for a disadvantage, this right would be of no use. So this right to privacy is a negative right to not be interfered with. Under it one does not have the right to be as private as one wishes, but only no less than the next person. Still, even this limited concept could be useful, if it were applied more rigorously.

Unfortunately, as the case law indicates, the right to privacy cedes too quickly to competing interests. An incomplete rough catalogue of these competing rights, drawn from the case law surveyed in this chapter include

a) public emergency and public safety (communications)
b) criminal investigation (search and seizure/communications)
c) competing private interests (divorce proceedings)
d) best interests of the child (paternity suits)
e) public interest (Right to Information)
f) competing fundamental rights (HIV status)

One may perhaps add judicial inactivity as one of the limiting factors on privacy.

By holding that violations of procedure by investigating agencies would not vitiate trials, the judiciary has been complicit in perhaps some of the more damaging incursions into privacy. Once a person is implicated in any manner in the criminal justice system – either as a victim, a witness or an offender, investigating agencies are immediately invested with plenary powers. They can search his house without warrant. They can place him arrest. Subject him to ‘medical examinations’ take his fingerprints and DNA and hold it in a bank and there is nothing you can do. In this context, perhaps the strongest privacy safeguard can come from a reform in criminal procedure alone.

Privacy is an individual as well as a social value. It is undoubtedly invaded everywhere at every moment due to the application of scientific and technological advances. Invasion of privacy and copyright violations are more in cyberspace though it is invisible. It has become very difficult to keep confidential information, communications anonymity etc., due to media interferences. Piracy is lucrative business now-a-days. However, the laws lag behind the digital revolution.