# Privacy In India - Country Report – October 2011

## §1 Core Country Information

India is the second-most populous country in the world with over 1.2 billion people according to the latest census (2011)[1]. It is the seventh-largest country in terms of geographical area.

The Constitution of India adopts a 'quasi-federal' structure of governance with a strong central (federal) government and relatively weaker sub-national 'states' - each with constitutionally designated spheres of legislative and executive authority. India follows a Parliamentary System of democracy with a bicameral legislature at the central level and in some states. An indirectly-elected President[2] serves as the constitutional Head of State. He is advised by a Prime Minister who is the Head of Government and the leader of the political party which wins a majority in the lower house of Parliament. Elections to the lower house of Parliament are conducted every five years.

The Indian Constitution envisages a unitary judicial structure with the Supreme Court at the apex and High Courts and subordinate courts at the state and sub-state level. Courts may exercise jurisdiction over matters covered by both federal and state laws and the higher judiciary is empowered to adjudicate constitutional issues. In addition, a range of administrative and quasi-judicial Tribunals and special courts also exists with jurisdiction limited to specified subjects – for instance the Income Tax Appellate Tribunal for Income Tax matters, or the Consumer Forums specially constituted to adjudicate consumer disputes.

India has had a strong tradition of civil society/NGO/Trade Union participation in demanding political accountability and NGOs have been active in pressing for change in all spheres –social, legal, economic and political.

According to latest available figures (July 2011), India has achieved a teledensity of 74% with over 892 million subscribers. Of these wireless subscribers account for 858 million.[3]

---

[1] Chapter 3: Size, Growth Rate and Distribution of Population, in Census of India: Provisional Population Totals 38 (2011), http://www.censusindia.gov.in/2011-prov-results/data_files/india/Final%20PPT%202011_chapter3.pdf (last visited Sep 23, 2011).

[2] The President of India is elected by an electoral college comprising all elected members of both houses of Parliament and elected members of the state legislative assemblies (Art 54 of the Constitution of India).

[3] Highlights of Telecom Subscription Data as on 31st July, 2011 (Press Release No. 47/2011), (2011), http://www.trai.gov.in/WriteReadData/trai/upload/PressReleases/837/Press_Release_July-11.pdf (last visited Sep 23, 2011).

## §2 The Legal Landscape for the protection of Privacy

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.

### 2.1 Constitutional protections for privacy

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 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.

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.

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, the Supreme Court has held in a celebrated case *Maneka Gandhi vs. Union of India*[4] 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."[5]

Notwithstanding this early setback, five decisions by the Supreme Court in the succeeding 5 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*[6] 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

[4] (1978) 2 SCR 621

[5] 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"

[6] (1964) 1 SCR 332

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 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 Subba Rao 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 Subba Rao’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 vs State Of Maharashtra*[7] 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.*”[8]

The third case in the series, *Govind vs. State of Madhya Pradesh*[9] (1975), 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 of the suspects. The Supreme Court desisted from striking down these invasive provisions holding that “It cannot be said that

[7] AIR 1973 SC 157, 1973 SCR (2) 417
[8] *Ibid*
[9] (1975) 2 SCC 148

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* onwards, '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*[10] (1980) 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 "unobstrusive 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 vs. State of Tamil Nadu*[11] (1994). 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 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

[10] AIR 1981 SC 760
[11] (1994) 6 S.C.C. 632

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 carved out to this rule, viz., 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*"[12]

The final case that makes up the 'privacy quintet' in India was the case of *PUCL v. Union of India*[13](1997), 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 ones 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."

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

[12] *Ibid*
[13] AIR 1997 SC 568

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.[14]

Thus, to conclude this section, 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 crime, or for the protection of health or morals, or for the protection of the rights and freedoms of others."[15]

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

[14] 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.

[15] Chapter 3: Fundamental Rights, Directive Principles And Fundamental Duties, *in* REPORT OF THE NATIONAL COMMISSION TO REVIEW THE WORKING OF THE CONSTITUTION (M.N. Venkatachaliah ed., 2002), http://lawmin.nic.in/ncrwc/finalreport/v1ch3.htm (last visited Oct 3, 2011).

## 2.2 Statutory protections for privacy

Although such a move is under consideration[16], India does not currently have a sui-generis statute that safeguards privacy horizontally across different contexts. However various statutes dealing with issues as diverse as banking and finance, professional ethics of lawyers, doctors and chartered accountants, information technology and telephony etc contain provisions which either explicitly or impliedly protect privacy and offer victims remedies for their breach. Details of some of these sector-specific privacy provisions are provided in later sections of this report. In this section we propose to deal mainly with privacy protections under the Information Technology Act, with special focus on Data Protection provisions and certain other miscellaneous laws which protect privacy.

### 2.2.1 The Information Technology Act

The Information Technology Act 2000 contains a number of provisions which can be used to safeguard against online/computer related privacy. The Act provides for civil and criminal liability with respect to hacking (Secs 43 & 66) and imprisonment of up to three years with fine for electronic voyeurism (Sec. 66E), Phishing and identity theft (66C/66D), Offensive email (Sec. 66A). Disclosure by the government of information obtained in the course of exercising its interception powers under the IT Act is punishable with imprisonment of up to two years and fine(Sec. 72) [17] Section 72A of the IT Act penalizes the unauthorized disclosure of "personal information" by any person who has obtained such information while providing services under a lawful contract. Such disclosure must be made with the intent of causing wrongful loss or obtaining a wrongful gain and is punishable with imprisonment which may extend to 3 years or a fine of Rs. 500,000 or both.

In addition to these sections, the Act also contains provisions with respect to Data Protection which are described below.

---

[16] Two different ministries of the Central Government are reportedly at work on drafts of a proposed privacy bill. In October 2010, the Department of Personnel and Training (DoPT), under the Ministry of Human Resources circulated an "Approach paper" that outlined elements of a privacy legislation for the country. Independent of this exercise, in May-June 2011, the Law Ministry announced that it was at work drafting a privacy bill "to provide for such a right [of privacy] to citizens of India AND to regulate collection, maintenance, use and dissemination of their personal information" Abantika Ghosh, *Right to privacy may become fundamental right*, TIMES OF INDIA, June 4, 2011,http://articles.timesofindia.indiatimes.com/2011-06-04/india/29620422_1_privacy-law-ministry-confidentiality (last visited Oct 3, 2011).

[17] For a more elaborate treatment of the IT Act's protections of privacy, and the manner in which they have been used, See Prashant Iyengar, *Privacy and the Information Technology Act in India*, SSRN ELIBRARY (2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1807575 (last visited Oct 3, 2011).

#### *2.2.1.1 Data Protection Liability for 'body-corporates' under Section 43A of the Information Technology Act and the Reasonable Security Practices Rules 2011*

Section 43A of the IT Act, newly introduced in 2008, makes a start at introducing a mandatory data protection regime in Indian law. The section obliges corporate bodies who 'possess, deal or handle' any 'sensitive personal data' to implement and maintain 'reasonable security practices', failing which, they would be liable to compensate those affected by any negligence attributable to this failure.

There are three key aspects of this section that bear highlighting:

- It is only the narrowly-defined 'body corporates'[18] engaged in 'commercial or professional activities' who are the targets of this section. Thus government agencies and non-profit organisations are entirely excluded from the ambit of this section[19].
- "Sensitive personal data or information" is any information that the Central Government may designate as such, when it sees fit to.
- The "reasonable security practices" which the section obliges body corporates to observe are restricted to such measures as may be specified either "in an agreement between the parties" or in any law in force or as prescribed by the Central Government.

In April 2011, the Ministry of Information and Technology, notified rules[20] under Section 43A in order to define "sensitive personal information" and to prescribe "reasonable security practices" that body corporates must observe in relation to the information they hold. By defining both phrases in terms that require executive elaboration, the section and the rules in effect pre-empt the courts from evolving an iterative, contextual definition of what would count as a reasonable security practice in relation to data. Various elements of these rules are discussed in the next sections.

---

[18] Section 43A defines "'body corporate" as any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

[19] This does not necessarily mean that these entities are exempt from taking reasonable care to safeguard information that they collect, maintain or control – only that remedies against the government must be sought under general tort law, rather than under the IT Act.

[20] The Information Technology (Reasonable security practices and procedures and sensitive personal information) Rules, 2011. Available at http://www.mit.gov.in/sites/upload_files/dit/files/GSR3_10511%281%29.pdf , last accessed September 15th, 2011

**Mphasis BPO Fraud: 2005**[21]

In December 2004, four call center employees, working at an outsourcing facility operated by MphasiS in India, obtained PIN codes from four customers of MphasiS' client, CitiGroup. These employees were not authorized to obtain the PINs.

In association with others, the call center employees opened new accounts at Indian banks using false identities. Within two months, they used the PINs and account information gleaned during their employment at MphasiS to transfer money from the bank accounts of CitiGroup customers to the new accounts at Indian banks.

By April 2005, the Indian police had tipped off to the scam by a U.S. bank, and quickly identified the individuals involved in the scam. Arrests were made when those individuals attempted to withdraw cash from the falsified accounts.

$426,000 was stolen; the amount recovered was $230,000.

## Sensitive Personal Information

Rule 3 of these Rules designates the following types of information as 'sensitive personal information':

(i) password;

(ii) financial information such as Bank account or credit card or debit card or other payment instrument details ;

(iii) physical, physiological and mental health condition;

(iv) sexual orientation;

(v) medical records and history;

(vi) Biometric information;

(vii) any detail relating to the above clauses as provided to body corporate for providing service; and

(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

[21] Anon, 2005. The MphasiS Scandal – And How it Concerns U.S. Companies Considering Offshore BPO. *Carretek*. Available at: http://www.carretek.com/main/news/articles/MphasiS_scandal.htm [Accessed March 29, 2011]. See also Anon, 2005. MphasiS case: BPOs feel need to tighten security. *Indian Express*. Available at: http://www.expressindia.com/news/fullstory.php?newsid=44856 [Accessed March 29, 2011].

## Mandatory Privacy Policies for body corporates

Rule 4 enjoins a body corporate or its representative who "collects, receives, possess, stores, deals or handles" data to provide a privacy policy "for handling of or dealing in user information including sensitive personal information". This policy is to be made available for view by such "providers of information"[22]. The policy must provide details of:

(i) Type of personal or sensitive information collected under sub-rule (ii) of rule 3;

(ii) Purpose, means and modes of usage of such information;

(iii) Disclosure of information as provided in rule 6[23].

## Prior Consent and Use Limitation during Data Collection

Body Corporates are forbidden by the rules from collecting sensitive personal information unless - (a) the information is collected for a lawful purpose connected with a function or activity of the agency; and (b) the collection of the information is necessary for that purpose.[24]

They and "any person" holding sensitive personal information are forbidden from "keeping that information for longer than is required for the purposes for which the information may lawfully be used"[25]

This however does not apply to "any information that is freely available or accessible in public domain or accessible under the Right to Information Act, 2005 or any other law for the time being in force.

In addition to the restrictions on collecting sensitive personal information, body corporate must obtain prior consent from the "provider of information. The body corporate is required to "take

[22] "Provider of data" is not the same as individuals to whom the data pertains, and could possibly include intermediaries who have custody over the data. We feel this privacy policy should be made available for view generally – and not only to providers of information. In addition, it might be advisable to mandate registration of privacy policies with designated data controllers.

[23] This is well framed since it does not permit body corporates to frame privacy policies that detract from Rule 6.

[24] Rule 5 of the Rules

[25] This is perhaps a bit vague, since the potential 'lawful uses' are numerous and could be inexhaustible. It is unclear whether "lawful usage" is coterminous with "the uses which are disclosed to the individual at the time of collection". In addition, this rule is framed rather weakly since it does not impose a positive obligation (although this is implied) to destroy information that is no longer required or in use.

such steps as are, in the circumstances, reasonable"[26] to ensure that the individual from whom data is collected is aware of :

(a) the fact that the information is being collected; and

(b) the purpose for which the information is being collected; and

(c) the intended recipients of the information; and

(d) the name and address of :

(i) the agency that is collecting the information; and

(ii) the agency that will hold the information.

During Data Collection, body corporates are required to give individuals the choice to opt-in or opt-out from data collection.[27] They must also permit individuals to review and modify the information they provide "wherever necessary"[28]. Information collected is to be kept securely[29], used only for the stated purpose[30] and any grievances must be addressed by the body corporate "in a time bound manner"[31].

Unlike "sensitive personal information" there is no obligation to retain other personal information only for as long as is it is required for the purpose collected.

### Limitations on Disclosure of Information

The Rules require a body corporate to obtain prior permission *from the provider of such information* obtained either "under lawful contract or otherwise" before information is disclosed.[32] The body corporate or any person on its behalf shall not publish the sensitive

[26] Sub-Rule 5(3). One wonders about the convoluted language used here when a simpler phrase like "take reasonable steps" alone might have sufficed - reasonableness has generally been interpreted by courts contextually. As the Supreme Court has remarked, "`Reasonable' means prima facie in law reasonable in regard to those circumstances of which the actor, called upon to act reasonably, knows or ought to know. *See* *Gujarat Water Supply and Sewage Board v. Unique Erectors* (Guj) AIR 1989 SC 973

[27] Sub-Rule 5(7)

[28] Sub-Rule 5(6). It is unclear what would count as a 'necessary' circumstance and who would be the authority to determine such necessity.

[29] Sub-Rule 5(8)

[30] Sub-Rule 5(5)

[31] Sub-Rule 5(9)

[32] Sub-Rule 6(1) There are two problems with this rule. First, it requires prior permission only from the provider of information, and not the individual to whom the data pertains. In effect this whittles down the agency of the individual in being able to control the manner in which information pertaining to her is used. Second, it is not clear whether this information includes "sensitive personal information". The proviso to this rule includes the phrase "sensitive information", which would suggest that such information would be included. This makes it even more

personal information.[33] Any third party receiving this information is prohibited from disclosing it further.[34]

However, this rule is subject to the exception that information is to be provided without prior consent to 'government agencies' for the purposes of "verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences". In such cases, the government agency is required to send a written request to the body corporate possessing the sensitive information, stating clearly the purpose of seeking such information. The government agency is also required to "state that the information thus obtained will not be published or shared with any other person"[35].

Sub Rule (2) of Rule 6 requires "any Information" to be "disclosed to any third party by an order under the law for the time being in force." This is to be done "without prejudice" to the obligations of the body corporate to obtain prior permission from the providers of information.[36]

Independent of these rules pertaining to 'disclosure', body-corporates may 'transfer' sensitive data or personal information without consent "to any other body corporate or a person in India, or located in any other country that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules". The transfer may be allowed only where it is determined to be "necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer" (Rule 7).

---

important that the rule require that prior permission be obtained from the individual to whom the data pertains and not merely from the provider of information.

[33] Sub-Rule 6(3)

[34] Sub-Rule 6(4)

[35] This is a curious insertion since it begs the question as to the utility of such a statement issued by the requesting agency. What are the sanctions under the IT Act that may be attached to a government agencies that betrays this statement? Why not instead, insert a peremptory prohibition on government agencies from disclosing such information (with the exception, perhaps, of securing conviction of offenders)?

[36] This sub-rule does not distinguish between orders issued by a court and those issued by an administrative/quasi-judicial body.

## Reasonable Security Practices

Rule 8 of the Rules stipulates that a body corporate shall be deemed to have complied with reasonable security practices if it has implemented security practices and standards which require
a) a comprehensive documented information security programme;
b) information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected.

In case of an information security breach, such body corporate will be "required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies".

The Rule stipulates that by adopting the International Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements", a body corporate will be deemed to have complied with reasonable security practices and procedures.

The Rule also permits "Industry associations or industry clusters" who are following standards other than IS/ISO/IEC 27001 but which nevertheless correspond to the requirements of Sub-Rule 7(1), to obtain approval for these codes from the government. Once this approval has been sought and obtained, the observance of these standards by a body corporate would deem them to have complied with the reasonable security practice requirements of Section 43A.

## Penalties and Remedies

Non-observance of the Data Protection Rules and general negligence with respect to personal data attracts civil liability.

As mentioned above, under Section 43A, any body corporates who fail to observe data protection norms may be liable to pay compensation if :

a) it is negligent in implementing and maintaining reasonable security practices, and thereby

b) causes wrongful loss or wrongful gain to any person[37];

In addition Section 45 of the Act provides for compensation or penalty of upto Rs. 25,000 to any person affected by the non-compliance with Rules framed under this Act (including the Data Protection Rules).

Claims for compensation are to be made to the Adjudicating Officer appointed under Section 46 of the IT Act.[38]

In addition, body corporates may also be exposed to criminal liability under Section 72A as described above, if they disclose information with the intent of causing wrongful loss or obtaining a wrongful gain.

## §3 Supervisory Authority for privacy laws and complaints

India does not have a national regulatory body to specially oversee the enforcement of privacy protections. However several sector-specific tribunals and adjudicatory authorities are empowered to determine issues of privacy that arise within their jurisdiction.

Thus, for instance, the State Information Commission and the Central Information Commission established under the Right to Information Act, 2005 adjudicate issues relating to privacy that arise in the course of requests for information under that Act. More than 700 decisions of the Central Information Commission between 2005 and 2011 directly reference the word 'privacy' – indicating that this is a frequent venue for the determination of a range of privacy issues in

[37] "Wrongful loss" and "wrongful gain" have been defined by Section 23 of the Indian Penal Code. Accordingly, "Wrongful gain" is gain by unlawful means of property which the person gaining is not legally entitled. "Wrongful loss"- "Wrongful loss" is the loss by unlawful means of property to which the person losing it is legally entitled." The section also includes this interesting explanation "Gaining wrongfully, losing wrongfully- A person is said to gain wrongfully when such person retains wrongfully, as well as when such person acquires wrongfully. A person is said to lose wrongfully when such person is wrongfully kept out of any property as well as when such person is wrongfully deprived of property". Following this, it could be possible to argue that the retention of data beyond the period of its use would amount to a "wrongful gain".

[38] For a more detailed discussion of redressal mechanism under the IT Act, including the powers of the Adjudicating Officer, see infra under 'Supervisory Authority for Privacy Law'

India.[39] The District, State and National Consumer Dispute Redressal Commissions can act as fora for the redressal of consumer privacy complaints.[40]

The Human Rights Act 1993 grants victims or their representatives the right to approach the Human Rights Commission for relief for the violation, or the negligence in the prevention of violation of a human right by a public servant (Section 12 of the HRA). Human rights have been defined in the Act to mean "the rights relating to life, liberty, equality and dignity of the individual guaranteed by the Constitution or embodied in" the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights. Since, as mentioned above, the right to privacy is considered a fundamental right attached to the right to life, and is also explicitly affirmed in Article 17 of the ICCPR, this is definitely a subject on which the Human Rights Commission could provide a forum for redress.

**Unlawful intercept**

In August 2007, Lakshmana Kailash K. a techie from Bangalore was arrested on the suspicion of having posted insulting images of Chhatrapati Shivaji, a major historical figure in the state of Maharashtra, on the social-networking site Orkut. The police identified him based on IP address details obtained from Google and Airtel – Lakshmana's ISP. He was brought to Pune and detained for 50 days before it was discovered that the IP address provided by Airtel was erroneous. The mistake was evidently due to the fact that while requesting information from Airtel, the police had not properly specified whether the suspect had posted the content at 1:15 pm or am.

Taking cognizance of his plight from newspaper accounts, the State Human Rights Commission subsequently ordered the company to pay Rs 2 lakh to Lakshmana as damages.[41]

The incident highlights how minor privacy violations by ISPs and intermediaries could

[39] See infra, 'Right to Information laws' for a discussion about this volume of cases.
[40] See §20.4 infra
[41] Holla, A., 2009. Wronged, techie gets justice 2 yrs after being jailed. *Mumbai Mirror*. Available at: http://www.mumbaimirror.com/index.aspx?page=article&sectid=2&contentid=20090625200906250314457868103 7483 [Accessed March 23, 2011].

have impacts that gravely undermine other basic human rights. [42]

Since the Information Technology Act contains the clearest provisions relating to Data Protection and Privacy in India, it would be instructive to examine briefly the enforcement mechanism under that Act. As noted above, violation of privacy and data protection under the Information Technology Act entails both civil and criminal remedies. We provide a brief overview of the adjudicatory apparatus for both.

## 3.1 Civil Complaints under the IT Act

Section 46 of the Information Technology Act empowers the Central Government to appoint "Adjudication Officers" to adjudicate whether any person has committed any of the contraventions described in Chapter IX of the Act (including contravention of the Data Protection Rules described in Section 2.2 above) and to determine the quantum of compensation payable. Accordingly, the Central Government has designated the Secretaries of the Department of Information Technology of each of the States or Union Territories as the "Adjudicating Officer" with respect to each of their territories.[43]

However, a pecuniary limit has been placed on the powers of Adjudicating Officers, and they may only adjudicate cases where the quantum of compensation claimed does not exceed Rs. 5 crores (Rupees Fifty Million). In cases where the compensation claimed exceeds this amount, jurisdiction would vest in the "competent court", under the Code of Civil Procedure. (Sec. 46A, IT Act) The AO is empowered with all the powers of a civil court – including the powers of summoning and enforcing attendance of witnesses, requiring the discovery and production of records, compounding complaints etc (Sec. 46, IT Act).

Although the powers of the AO under the Act are very extensive, they have been used very sparingly in the 11 years since the passage of the IT Act. No compilation of the orders of AOs of

[42] *See* also Nanjappa, V., 2008. 'I have lost everything'. *Rediff.com News*. Available at: http://www.rediff.com/news/2008/jan/21inter.htm [Accessed March 23, 2011].
[43] *See* G.S.R.240(E) New Delhi, the 25th March, 2003 available at < http://www.mit.gov.in/content/it-act-notification-no-240>

various states exists either online or offline and they are only sparingly reported in newspapers.[44] Among the cases that do get reported, however, there are encouraging signs of the Act being used to provide compensation to those who suffer due to data breaches by companies.

In April 2010, the Adjudicating Officer of the State of Tamil Nadu passed an order for compensation against a leading bank for its failure to install a foolproof internet banking system.[45] An amount of Rs. 4,60,000 had been illegally transferred out of the complainant's account and subsequently withdrawn by unknown persons. The AO observed that as a there was "unauthorized access to the petitioner's account.., loss of data and account information of the petitioner, damage to electronic information of the petitioner which resulted in financial loss, denial of access to his account". Further, the AO held that "The Respondent bank has failed to put in place a foolproof Internet Banking System with adequate levels of authentication and validation which would have prevented unauthorized access.. that has led to serious financial loss to the petitioner". Pursuant to this determination the respondent bank was ordered to pay an amount of Rs. 1,285,000 – which included the amount lost, interest, litigation expenses and travel expenses of the complainant.

In May 2011, the same bank was ordered by the same Adjudicating Officer to pay an amount of Rs. 237,850 for a similar incident where the complainant's money was illegally transferred out of his account.[46]

The IT Act provides for the constitution of a Cyber Appellate Tribunal to hear appeals from cases decided by the adjudicating officer.
Within twenty five days of the copy of the decision being made available by the Adjudicating Officer, the aggrieved party may file an appeal before the Cyber Appellate Tribunal.

Section 57 provides that the appeal filed before the Cyber Appellate Tribunal shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal

[44] Thus in a document dated December 2010, the IT Department of New Delhi (NCR) claimed that it had disposed of 5 cases. It is not clear whether this is the total number of cases ever decided or whether this only pertains to 2010. Govt. of NCT of Delhi: IT DEPARTMENT ACHIEVEMENTS (Legal Section), (2010), http://goo.gl/GEq26 (last visited Oct 3, 2011).
[45] Umashankar v. ICICI Bank, Tuticorin, (2010), http://www.naavi.org/cl_editorial_10/umashankar_judgement.pdf (last visited Sep 26, 2011
[46] Thomas Raju v. ICICI Bank, Anna Nagar, (2011), http://www.naavi.org/cl_editorial_11/civil_jurisdiction_3_16052011.pdf (last visited Sep 26, 2011).

finally within six months from the date of receipt of the appeal. According to the Tribunal's website, the CAT currently has 12 cases listed as 'pending' before it.[47] It has disposed 8 cases, 7 of which were disposed on the same day[48] – May 26 2010 – and in every case, the case was remanded back to an Adjudicating Officer for determination of facts. Some of these cases complain of privacy violations or seek reliefs which have implications on privacy. For instance, in *Mascon Global Limited V. CCA, Google etc*, disposed by the CAT on May 28, 2010, the appellant had sought details about an email account from Google which was purportedly being used to send defamatory emails. The CAT remanded the case to the Adjudicating Officer, which according to it was the appropriate forum to decide the case. [49] In another case, widely reported in the press, a man filed a complaint of hacking against his estranged wife alleging that she had, with the aid of her professional colleagues, hacked into his and his father's email account in order to obtain evidence in support of a dowry harassment case that she had filed against them.[50] The Adjudicating Officer in the first instance had dismissed the complaint believing her assertion that the man and his father had themselves given her the password– a contention which was not denied by the complainant.[51] On appeal, however, the man contended that he had not, in fact, given his wife the password. The CAT ordered the case to be re-heard by the AO.[52] Although the complaint alleged 'hacking' by the woman, the case in fact refers to a privacy grievance of the complainant.

Section 62 gives the right of appeal to a High Court to any person aggrieved by any decision or order of the Cyber Appellate Tribunal on any question of fact or law arising out of such order.

---

[47] Current Cases, CYBER APPELLATE TRIBUNAL, INDIA (2011), http://catindia.gov.in/CurrentCases.aspx (last visited Oct 3, 2011).
[48] Judgments, CYBER APPELLATE TRIBUNAL, INDIA (2011), http://catindia.gov.in/Judgement.aspx (last visited Oct 3, 2011).
[49] Mascon Global Limited v. CCA, Google etc,, (2010), http://www.mit.gov.in/sites/upload_files/dit/files/Appeal-7.pdf (last visited Oct 3, 2011).
[50] Mubarak Ansari, *Estranged wife hacks man's email*, SAKAL TIMES, August 25, 2011, http://www.sakaaltimes.com/sakaaltimesbeta/20110825/4640115296625293785.htm (last visited Oct 3, 2011).
[51] *Ibid*
[52] Vinod Kaushik v. Madhvika Joshi, (2011), http://catindia.gov.in/pdfFiles/Appeal_No_2.pdf (last visited Oct 3, 2011).

## 3.2 Criminal Complaints for privacy offences under the IT Act

No special procedure is prescribed for the trial of cyber offences and hence the general provisions of criminal procedure would apply with respect to investigation by the police, charge sheet, trial, decision, sentencing and appeal.

Section 78 of the IT Act empowers police officers of the rank of Inspectors and above to investigate offences under the IT Act.Many States have set up dedicated Cyber Crime Police Stations to investigate offences under this Act[53]. Thus, for example, the State of Karnataka has set up a special Cyber Crime police station that is responsible for investigating all offences under the IT Act with respect to the entire territory of Karnataka.[54]

Offences punishable with imprisonment up to 3 years are compoundable by a competent court. However repeat offenders cannot have their subsequent offences compounded. Additionally, offences which "affect the socio-economic conditions of the country" or those committed against a child under 18 years of age or against women cannot be compounded.[55]

According to the latest (2009) statistics from the National Crime Records Bureau, there has been a steady rise in the number of complaints lodged and arrests made (both privacy and non-privacy related) with respect to offences under the IT Act.[56] In 2009, for instance, 420 complaints were registered, as against a figure of 288 for the previous year marking an increase of 41%. In the same period, the number of arrests made went up from 178 to 288 marking an increase of 41%.[57]

Of these, the NCBR categorizes 10 complaints in 2009 as pertaining to 'Breach of confidentiality/privacy' as against 9 complaints in the previous year. 5 arrests were made in 2009 with respect to these offences. However this figure does not exhaust the number of privacy complaints in the country since, in many cases, violations of privacy may result from 'Hacking

---

[53] An incomplete list of cyber crime cells of police in different states can be viewed at <http://infosecawareness.in/cyber-crime-cells-in-india>.

[54] Home and Transport Secretariat, Notification no. HD 173 POP 99 Bangalore, Dated 13th September 2001 Available at < http://cyberpolicebangalore.nic.in/pdf/notification_1.pdf>

[55] Section 77A of the Information Technology Act.

[56] CRIME IN INDIA - 2009, (2010), http://ncrb.nic.in/CII-2009-NEW/Compendium2009.pdf (last visited Oct 3, 2011).

[57] *Chapter 18: Cyber Crime*, *in* CRIME IN INDIA - 2009 175-180 (2010), http://ncrb.nic.in/CII-2009-NEW/Compendium2009.pdf (last visited Oct 3, 2011).

with a computer system' which, according to NCBR statistics, accounted for the largest number of complaints (233) and arrests (107) made under the IT Act in 2009.

## §4 Awareness of privacy: Outstanding civil society advocacy

Awareness of privacy issues is on the rise within NGOs, academic institutions and media organizations in India. As mentioned above, one of the most influential judgments by the Supreme Court of India on the issue of wiretapping was brought to it in 1997 as a Public Interest Litigation by the People's Union of Civil Liberties – an acclaimed NGO working on civil rights issues in India. In 2009, the Delhi High Court, in a major ruling, 'read down' Section 377 of the Indian Penal Code which had been previously used to criminalize homosexuality in India. A major plank of the ruling was an affirmation of the citizen's right to privacy which the court upheld as fundamental. This case was also brought to the Delhi High Court as a PIL by an NGO called the Naz Foundation. So NGOs have played a pivotal role in shaping the right to privacy in India over the years. In addition organisations like the Center for Internet and Society in Bangalore have played a part in raising awareness among government and the public about online privacy issues.

More recently, since November-2010 there has been renewed interest and public discussion about issues of communications privacy owing to a major controversy called the 'Radia tapes' expose. In mid-November 2010, two leading newspapers published wiretapped telephonic conversations between Nira Radia, a noted corporate lobbyist, and several influential Indians including the heads of several powerful media companies, and multi national companies. The conversations had been tapped by the Income Tax Department in the course of their investigation into her finances, and are widely regarded as exposing a shameful nexus between business, media and politics in India. Ratan Tata, one of the industrialists whose conversation with Radia was published, has filed a case in the Delhi High Court seeking an injunction against the publication of these tapes on grounds of violation of his 'right to privacy'. This controversy has churned a debate on the conditions under which wiretapping may be lawfully conducted, and the uses to which such information may be put. Although not the first instance of this kind, the controversy provides an immediate and emotive fulcrum to anchor discussion concerning issues of privacy and transparency that our study aims to raise.

In addition, in 2010, India embarked on an ambitious scheme of issuing Unique Identity (UID) cards to over half a billion people by the year 2014. In terms of its scale, this scheme is unprecedented in the world with the aiming to photograph 600 million Indians, "scan 1.2 billion irises, collect six billion fingerprints and record 600 million addresses"[58] before 2014. There has been spirited opposition from civil society to the scheme on grounds, among others, of the privacy concerns it raises, and a number of influential activists have been voicing their opposition in print and at consultations. Perhaps one of the most energetic campaigners against the scheme has been Usha Ramanathan, a senior independent law researcher and activist who has written extensively against the scheme, lobbied with Parliamentarians and spoken at numerous fora across the country.[59] Her efforts have led to a greater appreciation of privacy among NGOs and activist groups in India. In addition various widely led blogs and discussion forums such as The Hoot and MediaNama have been instrumental in raising awareness of privacy in the context of the media.

In recent times, media organizations have also begun to pay greater attention to privacy concerns. The broadcast industry has set up a self-regulatory organization – that News Broadcasting Standards Authority (NBSA) - with a Code of Ethics which explicitly obliges channels not to intrude on "private lives, or personal affairs of individuals, unless there is a *clearly established larger and identifiable public interest* for such a broadcast". In March 2005, the NBSA slapped a 1 lakh rupee fine on the news channel TV9 for airing an extremely incendiary and invasive programme titled "Gay Culture rampant in Hyderabad" which used phone numbers from a social-networking site for gay men to 'entrap' youth into admitting their sexual preferences on the air.[60] In addition the channel was required to display a public apology on prime time. This is a welcome sign that the broadcast industry is willing to back its ethical commitment to privacy with swift remedies.

---

[58] Jayashankar, Mitu, and N.S. Ramnath. "UIDAI: Inside the World's Largest Data Management Project." *Forbes India*, December 3, 2010. http://business.in.com/article/big-bet/uidai-inside-the-worlds-largest-data-management-project/19632/1

[59] *See* for instance Usha Ramanathan, *A private right or a public affair?*, 8 TEHELKA, 2011, http://www.tehelka.com/story_main50.asp?filename=Ne090711PROSCONS.asp (last visited Oct 3, 2011).

[60] Prashant Iyengar, NEWS BROADCASTING STANDARDS AUTHORITY CENSURES TV9 OVER PRIVACY VIOLATIONS! PRIVACYINDIA (2011), http://privacyindia.org/2011/03/25/news-broadcasting-standards-authority-censures-tv9-over-privacy-violations/ (last visited Oct 3, 2011).

Despite a growing awareness of privacy among academicians, this sensibility has not filtered upwards to the institutions they represent. In February 2010, in a much publicized case, a senior professor of Aligarh Muslim University – one of the oldest in the country – was suspended after students "set up cameras to catch him having consensual sex with a rickshaw-puller in his campus home".[61] Many universities and schools in India have installed extensive CCTV camera networks on their premises. In January 2011, the Maharashtra Government passed a resolution requiring all universities in the state to install a biometric card system on their campus.[62] In February 2011, fingerprint data was captured from over 11,000 aspirants writing an entrance exam for Post Graduate medical admissions in the state of Karnataka.[63] In September 2011, the West Bengal Government ordered all undergraduate college campuses in the state to install CCTV camera networks.[64] So it certainly appears as if administrative insensitivity to privacy in academic spaces has kept with pace with the growing sensitivity among academics to the issue.

## §5 Freedom of information laws

India has had the good fortune of being home to a number of very resilient civil society movements which have over the years tenaciously fought for and achieved transparency. It was owing to the efforts of one of these movement spearheaded by the Mazdoor Kisan Shakti Sanghatan (MKSS) and joined by various organizations across the nation[65], that India finally passed the Right to Information Act in 2005, which has ushered in an unprecedented era of openness in government affairs.

The RTI Act 2005 confers on citizens the right to inspect and take copies of any information held by or under the control of any 'public authority'[66]. Information is defined widely and includes

[61] Manjari Mishra, *Aligarh Muslim University professor suspended for being gay*, TIMES OF INDIA, February 18, 2010, http://articles.timesofindia.indiatimes.com/2010-02-18/india/28118769_1_shrinivas-ramchandra-siras-rickshaw-puller-amu-campus (last visited Oct 3, 2011).

[62] Yogita Rao, *Maharashtra colleges to install biometric card systems to check attendance - Mumbai - DNA*, DNA INDIA, January 14, 2011, http://www.dnaindia.com/mumbai/report_maharashtra-colleges-to-install-biometric-card-systems-to-check-attendance_1494247 (last visited Jan 18, 2011).

[63] Biometrics Employed to Crack down on Proxies, THE HINDU, February 7, 2011, http://www.hindu.com/2011/02/07/stories/2011020756020700.htm (last visited Oct 3, 2011).

[64] It's official: colleges on camera -Circular asks principals to install CCTVs to check unrest & illicit activity, THE TELEGRAPH, September 21, 2011, http://www.telegraphindia.com/1110921/jsp/calcutta/story_14532267.jsp (last visited Oct 3, 2011).

[65]

[66] 'Public authority' is defined widely to include most bodies established and constituted by the state and even bodies which are 'owned, controlled or substantially financed' by the state. [Sec 2(h)]

"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". The Act requires every 'public authority' to designate an officer in *each* of its administrative units as 'Public Information Officer' (PIO) who is charged with the task of receiving and responding to requests under this Act.

The drafters of the Act anticipated conflicts on grounds of privacy. The Preamble to the Act notes that 'revelation of information in actual practice is likely to conflict with other public interests including.. preservation of confidentiality of sensitive information". Accordingly, provisions have been made in the Act to harmonizing these competing claims to the extent possible.

Section 8 (j) of the Act exempts from disclosure any "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". Further, Section 11 of the Act requires the PIO to give notice and invite objections from a third party, if information which "relates to or has been supplied by a third party and has been treated as confidential by that third party" is sought to be disclosed. Objections received from such parties would be considered whilst making a decision to disclose. Even where objections have been received, disclosure may be allowed if public interest outweighs in importance any possible harm or injury to the interests of such third party. However, trade or commercial secrets protected by law may not be disclosed notwithstanding any public interest.

Persons who have been denied information on the above grounds have the option to appeal this decision before the next higher ranking officer to the PIO, and thereafter to specially constituted tribunals under the Act – the State Information Commission and the Central Information Commission. At each stage, if information has been denied on grounds that it relates to third parties, the third party in question must give a reasonable hearing to the third party.

As is evident from the foregoing account, the Act has put in place a robust buffer against unwarranted intrusion. Personal information, the disclosure of which would cause an 'unwarranted' intrusion into privacy, and information which 'relates to a third party' may not be disclosed unless an overwhelming countervailing public interest is demonstrated.

More than providing mere statutory comforts, these provisions have proven, in practice, to be rugged shelters against unwarranted attempts to intrude on privacy. In the six years since the enactment of the RTI Act, over *seven hundred* decisions by the Central Information Commission alone directly reference the term 'privacy'.

Illustratively, in the following instances, the CIC has denied requests for information on grounds of unwarranted intrusion of privacy: where call records of third parties were requested[67], copies of 'annual confidential reports' of other employees[68], bank statements of a partner of a firm[69], copy of a CBI charge sheet against an officer of an organization[70], details of all passengers who were on a particular flight[71], income tax returns of a third party[72], specimen signature of a third person[73], medical records of the appellant's wife[74], number of employees of an organization who had committed suicide[75] etc.

In a famous case 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

[67] Mr.S.Rajamohan v Bsnl, Chennai, (2009), http://indiankanoon.org/doc/1864526/ (last visited Oct 12, 2011).
[68]
[69] Ms. Kanchan Vora v Union Bank Of India, (2008), http://indiankanoon.org/doc/456808/ (last visited Oct 12, 2011).
[70] Shri P. Thavasiraj v Dept. Of Atomic Energy, (2008), http://indiankanoon.org/doc/1718696/ (last visited Oct 12, 2011).
[71] K.P. Subhashchandran v National Aviation Company, (2008), http://indiankanoon.org/doc/1067875/ (last visited Oct 12, 2011).
[72] Mrs.Shobha R. Arora v. Income Tax (2006), Mumbai, Ms. Neeru Bajaj Vs. Income Tax (2007), Bimal Kanti Datta v Income Tax Department, (2008), http://indiankanoon.org/doc/292462/ (last visited Oct 12, 2011).
[73] M.Nagaraju v Department Of Post (2008), http://indiankanoon.org/doc/215697/ (last visited Oct 12, 2011).
[74] Dheeraj Gehani v Ministry Of Defence (2009), http://indiankanoon.org/doc/163722/, (last visited Oct 12, 2011).
[75] Shri.Chetan Kothari vs Bhabha Atomic Research Centre (2011), http://indiankanoon.org/doc/425930/ (last visited Oct 12, 2011).

Punjab and Haryana High Court upheld the denial of information as it would otherwise lead to an unwarranted incursion into her privacy. [76]

In several cases, the CIC has astutely balanced the competing interests of transparency and privacy and has ordered disclosure where public interest was manifestly at issue. The CIC has ordered disclosure of a list of public servants being prosecuted for offences by the Central Vigilance Commission[77]. It has ordered disclosure of details of the number of beneficiaries from a particular village under a loan scheme and amount disbursed by a public sector bank, whilst ordering the names of the beneficiaries to be withheld[78]. Students have been able to obtain copies of their mark sheets in public exams.[79]

As welcome as these rulings are, there are however, a number of disconcerting cases where the determination has raised questions of privacy. In an interesting case *Mr.Ansari Masud A.K vs Ministry Of External Affairs* (2008)[80], the Central Information Commission 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."[81] This is despite the fact that nothing in the Passport Act itself authorizes disclosure of any documents under any circumstances. In another

[76] High Court dismisses appeal seeking information on Sonia Gandhi's religion, NDTV, November 29, 2010, http://www.ndtv.com/article/india/high-court-dismisses-appeal-seeking-information-on-sonia-gandhi-s-religion-69356 (last visited Apr 12, 2011)

[77] Shruti Singh Chauhan v Directorate Of Vigilance, (2008), http://indiankanoon.org/doc/1128532/, /(last visited Oct 12, 2011). Holding that "Information about alleged wrongdoing of Public servants,- verified by a process of investigation,- cannot be termed as private information which must be hidden from the Sovereign Masters of this democracy- the Citizens."

[78] Madasamy v State Bank Of India(2008), http://indiankanoon.org/doc/1430405/, (last visited Oct 12, 2011).

[79] Mr. D. Radha Krishna v. Union Public Service Commission (2008), http://indiankanoon.org/doc/1822201 (last visited Oct 12, 2011).

[80] .Ansari Masud A.K v Ministry Of External Affairs (2008) http://indiankanoon.org/doc/1479476/, (last visited Oct 12, 2011). In a previous case, the CIC ordered disclosure of passport details of a doctor against whom there had been allegations of medical malpractice. Sanjiv Kumar Jain v Regional Passport Office, (2006), http://indiankanoon.org/doc/1888134/ (last visited Oct 12, 2011).; Mr.Pritpal Singh Sawhney v. Ministry Of External Affairs (2011), http://indiankanoon.org/doc/1773560, (last visited Oct 12, 2011).

[81] *Id*

case, the CIC ordered, overruling the objection of the PIO of the university, disclosure of the names, nationalities and results of all foreign students admitted to the Delhi University.[82]

The CIC has dithered in formulating a uniform theory on what counts as 'personal information', disclosure of which would amount to an 'unwarranted intrusion into privacy'. It has, in different contexts, forbidden the revelation of individuals' names as intrusive[83], while permitting disclosure in others cases. [84] Details of criminal prosecution of co-employees have on different occasions been either disclosed[85] or withheld[86]. In cases where it has achieved a consistence in rulings, the determination is frequently adverse to privacy. For instance, there is by now a strong line of CIC decisions permitting the disclosure of passport details of third parties[87], qualifications (including copies of certificates) of co-workers[88],

Since 2009, the CIC – or more accurately Shailesh Gandhi, one of the Information Commissioners of the CIC - has attempted to formulate a coherent theory on what constitutes 'personal information' under the RTI Act. In one of his more recent decisions, *Mr.V R Sharma v Ministry Of Labour And Employment*[89], he reiterated his position[90] that in order to qualify as 'personal information', certain criteria would have to be met:

> 1. It must be personal information: Words in a law should normally be given the meaning given in common language. In common language, we would ascribe the adjective 'personal' to an attribute which applies to an individual and not to an institution or a

[82] Amit Chamaria v University Of Delhi (2008) http://indiankanoon.org/doc/98221/ (last visited Oct 12, 2011).
[83] *See* Madasamy v State Bank Of India, supra; Mr. Satish Kumar v.Union Public Service Commission (2011) http://indiankanoon.org/doc/882947 (last visited Oct 12, 2011). (Ordering disclosure of marks lists of successful candidates without revealing their names)
[84] Ms. Usha Rao v University Of Hyderabad (2008), http://indiankanoon.org/doc/836580/(last visited Oct 12, 2011). (Ordering the names of members of a selection panel constituted to appoint a Hindi lecturer to be revealed). See also Amit Chamania's case supra. Prof. Harish Chandra v Banaras Hindu University, (2008), http://indiankanoon.org/doc/1302334, (last visited Oct 12, 2011) (ordering the revelation of names of recipients of a deceased colleague's pension)
[85] *See* Shruti Singh Chauhan's case *supra*.
[86] *See* Thavasiraj's case *supra*, *See also*, Mr. K. C. Panday v. Municipal Corporation Of Delhi, (2008), http://indiankanoon.org/doc/959771 (last visited Oct 12, 2011). (Disclosure of whether Vigilance clearance has been obtained with regard to all emloyees)
[87] *See* Supra n. 79 and accompanying text
[88]M. Rajamannar v IGNOU (2009) http://indiankanoon.org/doc/1312655, (last visited Oct 12, 2011) (Ordering the delivery of copies of third persons' educational certificates)
[89] Mr.V R Sharma vs Ministry Of Labour And Employment (2011), http://indiankanoon.org/doc/1640569/ (last visited Oct 12, 2011).
[90] As of this writing, the same paragraphs have been quoted identically in some 78 decisions of the CIC by Shailesh Gandhi. beginning in *Mr. Mahesh Kumar Sharma v Govt. Of Nct Of Delhi*

Corporate. Therefore, it flows that 'personal' cannot be related to institutions, organisations or corporates. Hence Section 8(1)(j) of the RTI Act cannot be applied when the information concerns institutions, organisations or corporates.

2. The phrase 'disclosure of which has no relationship to any public activity or interest' means that the information must have been given in the course of a public activity. Various public authorities in performing their functions routinely ask for 'personal' information from citizens, and this is clearly a public activity. Public activities would typically include situations wherein a person applies for a job, or gives information about himself to a public authority as an employee, or asks for a permission, licence or authorisation, or provides information in discharge of a statutory obligation.

3. The disclosure of the information would lead to unwarranted invasion of the privacy of the individual. The State has no right to invade the privacy of an individual. There are some extraordinary situations where the State may be allowed to invade the privacy of a citizen. In those circumstances special provisions of the law apply usually with certain safeguards. Therefore where the State routinely obtains information from citizens, this information is in relationship to a public activity and will not be an intrusion on privacy.

In the instant case, the CIC applied this formula to permit the disclosure of Annual Confidential Reports of certain employees of the Ministry Of Labour And Employment. In the course of its decision, the CIC also made some worrying observations about the balance between privacy and transparency. “The concept of 'privacy' ”, it observed, “is a cultural notion related to social norms, and different societies would look at these differently. Therefore referring to the Data Protection Act, 1988 of U. K. or the laws of other countries to define 'privacy' cannot be considered a valid exercise to constrain the citizen's fundamental right to information in India. Parliament has not codified the right to privacy so far, hence, *in balancing the right to information of citizens and the individual's right to privacy, the citizen's right to information would be given greater weightage*.” (emphasis added). As a statement of policy this last assertion has worrying implications, since it could potentially undo the delicate balance between transparency and privacy that Parliament sought to put in place through the RTI Act. Equally the CIC’s bald assertion that all information ‘routinely collected by the state’ would not be intrusive is menacing especially in this era of the ‘ethnographic state’ which believes in maintaining

minute details about each of its citizens. Although the other four Information Commissioners have not adopted this formula yet, it is possible that by dint of repetition, it may sediment itself to become an axiom of CIC jurisprudence.

While there are statutory mechanisms protecting the privacy of citizens under the Right to Information Act, unfortunately this does not provide them a complete shield against transparency – this is particularly evident in the case where the state embarks on transparency initiatives of its own invention. Several states for instance have websites with lists of citizens in various contexts such as employment guarantee and public distribution systems.[91] In one particularly egregious instance, the State Government of Karnataka, overcome in its enthusiasm to weed out duplicate ration cards and promote transparency, announced a plan to "post on its website all details of (1.51 crore) ration cardholders in the state" These details posted on the website would include the "ration card number, category of card (BPL/APL), names and photographs of the head and other members of a family, address, sources of income, LPG gas connection and number of cylinders in village/taluk/district wise." One is even uncertain whether this following remark by an official, quoted in the newspaper account, was meant purely in jest: "This would also work as a marriage bureau. "For instance, a boy can see a photograph of a girl on the website and see whether she suits him," an official said".[92]

While the RTI Act provides an important safeguard against the violation of privacy, with official avenues for redress for the citizen, ad hoc 'transparency' initiatives of this kind leave the citizen with absolutely no recourse. There are, sadly, no statutory safeguards against the oppressive transparency of the state. It is unimpeachable (except possibly through writ petitions) decisions of this kind, rather than the threats under the RTI Act which pose a real 'transparency' threat to privacy in India.

## §6 International obligations pertaining to privacy

India is a signatory to the International Covenant on Civil and Political Rights which explicitly affirms the right to privacy in Article 17. As noted previously in this report, the Human Rights

[91] Ayaskant Das, *Ration card details now online to prevent fake registration*, TIMES OF INDIA, September 24, 2011, http://timesofindia.indiatimes.com/city/noida/Ration-card-details-now-online-to-prevent-fake-registration/articleshow/10099236.cms (last visited Oct 23, 2011).

[92] Nagesh Prabhu, *A way to check bogus ration cards*, THE HINDU, September 18, 2010, http://www.thehindu.com/todays-paper/tp-national/tp-karnataka/article696087.ece (last visited Oct 23, 2011).

Act expressly permits individuals to approach the National Human Rights Commission or any of the State Human Rights Commissions for redress of human rights infringed under this convention.

Apart from this, there are no regional conventions that deal specifically with privacy.

India has signed and ratified the International Convention for the Suppression of Terrorist Bombings[93] and the International Convention for the Suppression of the Financing of Terrorism.[94] India is a signatory to the SAARC Convention on Mutual Assistance in Criminal Matters as well as several bilateral treaties on mutual legal assistance. These treaties typically requires signatory states to provide mutual assistance in criminal matters, including, *inter alia*, "providing information, documents and records;" "providing objects, including lending exhibits", "search and seizure" , "taking evidence and obtaining statements;" etc. [95]

India is a signatory to 85 agreements (81 DTAAs and 4 TIEA agreements) on exchange of tax information. For instance, India has reportedly signed four Tax Information Exchange Agreements (TIEAs) on the OECD Model each with the Governments of the Bahamas, Bermuda, Cayman Islands and the Isle of Mann[96] – popular 'tax havens'. These agreements enjoin the 'competent authorities' of each country to provide information 'upon request' about a variety of financial details including bank records and corporate information. [97] The request must be made on the basis of evidence and fishing expeditions are not usually permitted. These agreements include standard Confidentiality clauses which require that the information only be

[93] Signed and ratified respectively on the 17th and 22nd of September 1999. International Convention for the Suppression of Terrorist Bombings, UN TREATY CENTER (2011), http://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-9&chapter=18&lang=en (last visited Oct 9, 2011).

[94] Signed and ratified respectively on 8 Sep 2000 and 22 Apr 2003 International Convention for the Suppression of the Financing of Terrorism, UN TREATY CENTER (2011), http://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-11&chapter=18&lang=en (last visited Oct 9, 2011).

[95] SAARC CONVENTION ON MUTUAL ASSISTANCE IN CRIMINAL MATTERS (2008), http://goo.gl/Wg5OM (last visited Oct 24, 2011).

[96] *India: Agreements*, EXCHANGE OF TAX INFORMATION PORTAL, OECD , http://www.eoi-tax.org/jurisdictions/IN#agreements (last visited Oct 24, 2011); *Tax Information Exchange Agreements (TIEAs)*, CENTER FOR TAX POLICY AND ADMINISTRATION, OECD , http://www.oecd.org/document/7/0,3746,en_2649_33767_38312839_1_1_1_1,00.html (last visited Oct 24, 2011).

[97] *See for instance*, AGREEMENT BETWEEN THE GOVERNMENT OF THE COMMONWEALTH OF THE BAHAMAS AND THE GOVERNMENT OF THE REPUBLIC OF INDIA FOR THE EXCHANGE OF INFORMATION WITH RESPECT TO TAXES (2011), http://www.oecd.org/dataoecd/47/54/47115735.pdf (last visited Oct 24, 2011).

disclosed to appropriate tax authorities for purposes of tax proceedings. They also exempt information disclosed to an attorney under attorney client privilege from being disclosed.[98]

In addition, India has signed a number of Double Taxation Avoidance Agreements which include information-sharing clauses. In June 2010, the Government approached the governments of 65 countries to "specifically" provide for the sharing of bank-related information.[99] Pursuant to this, most notably, in June 2011, the Indian Government entered into a revised DTAA with the Swiss government allowing India to "gain access to the details of Indians' money, which is not accounted for, stashed in Swiss banks".[100] Similarly, in the same month, the government of Mauritius agreed to renegotiate its tax treaty with India. Mauritius accounts for more than 40% of total foreign direct investments (FDIs) to India most of which are suspected to be nothing more than treaty shopping arrangements to avoid paying tax.[101] An OECD report on India's current DTA with Mauritius points to vast 'gaps' in the treaty including provisions requiring 'disclosure of information to the persons in respect to whom information or document had been sought' and that Mauritius has not exchanged information over the last three years.[102]

These treaties seem to have resulted in some information being shared. In October 2011, Pranab Mukherjee, the Finance Minister reported that, pursuant to these treaties, "Specific requests in 333 cases… have been made by Indian authorities for obtaining information from foreign jurisdictions. Over 9,900 pieces of information regarding suspicious transactions by Indian citizens from several countries have been obtained which are now under different stages of investigation,"[103]

---

[98] *Id.*

[99] *Govt revises tax information exchange treaty with 65 countries*, ECONOMIC TIMES, June 27, 2010, http://articles.economictimes.indiatimes.com/2010-06-27/news/27596832_1_dtaa-double-taxation-avoidance-agreement-check-tax-evasion (last visited Oct 24, 2011).

[100] *India, Switzerland ink pact to cooperate on financial matters to better analyze global econ developments*, CONTIFY BANKING (2011), http://banking.contify.com/story/india-switzerland-ink-pact-to-cooperate-on-financial-matters-to-better-analyze-global-econ-developments-2011-10-07 (last visited Oct 24, 2011).

[101] *Mauritius agrees to revise tax treaty*, TIMES OF INDIA, June 19, 2011, http://articles.timesofindia.indiatimes.com/2011-06-19/india/29676414_1_treaty-shopping-tax-havens-dtaas (last visited Oct 24, 2011).

[102] Sidhartha, *India's DTAA with Mauritius has gaps, says OECD study*, TIMES OF INDIA, January 29, 2011, http://articles.timesofindia.indiatimes.com/2011-01-29/india-business/28375723_1_limitation-of-benefit-clause-mauritius-mauritian (last visited Oct 24, 2011).

[103] *'Government successful in unearthing black money'*, THE HINDU, October 19, 2011, http://www.thehindu.com/news/national/article2551810.ece?homepage=true (last visited Oct 24, 2011).

Although information obtained under DTAAs cannot be used for purposes other than tax proceedings, in June 2011, the Income Tax Department announced that it would re-negotiate this clause in its agreements to enable it to share information with other law enforcement agencies like the Central Bureau of Investigation and the Enforcement Directorate.[104]

## §7 Law Enforcement and National Security

Technically, any law that authorizes the production of documents, search and seizure can be said to be one related to "lawful access". The two main procedural laws in India – the Code of Civil Procedure (CPC), and the Criminal Procedure Code (CrPC), both contain detailed provisions to compel the production of documents from parties to suits and criminal proceedings and witnesses. In addition, many other laws provide for the production of documents, searches and seizure, on various grounds - ranging from the Income Tax Act which authorizes Income Tax officials to issue summons for the production of documents and conduct searches to recover undisclosed income[105], 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 very briefly with the general provisions for the production of documents under the CPC and the CrPC.

### 7.1 Production of documents in Civil cases

Section 30 of the CPC empowers courts to make orders relating to discovery and issue summonses to persons (witnesses or parties) to produce documents.

Order XI of the CPC sets down procedures relating to 'Discovery' and provides for a party to compel the opposite party to list documents held in their possession "relating to any matter in question in such suit", to afford facilities to inspect them and to produce them in Court. The Court may also order copies of documents held in one party's possession to be delivered to the

[104] Bijay Shankar Patel, *I-T dept plans to share DTAA information*, FINANCIAL EXPRESS, June 7, 2011, http://www.financialexpress.com/news/it-dept-plans-to-share-dtaa-information/800119/1 (last visited Oct 24, 2011).

[105] Section 131 of the Income Tax Act, for instance, empowers Income Tax authorities with all the powers of a Civil Court for the purposes of discovery. An Income Tax officer may exercise these powers if he has "reason to suspect that any income has been concealed, or is likely to be concealed, by any person or class of persons". Under Section 132 of the Income Tax Act, a search (and seizure) may be ordered by an Income Tax officer if he, "in consequence of information in his possession, has reason to believe" that the document summoned is not likely to be produced. The section also empowers the Income Tax Officer to require any person in possession of books (of accounts) maintained electronically to "afford the authorised officer the necessary facility to inspect such books of account or other documents".

other party. If a plaintiff fails to comply with an order for the discovery of documents, then his suit may be liable to be dismissed for want of prosecution. Similarly, if a defendant fails to comply, he would be liable "to have his defence, if any struck out, and to be placed in the same position as if he had not defended". In this context, the Supreme Court has held that "the power to order production of documents is coupled with discretion to examine the expediency, justness and the relevancy of the documents to the matter in question."[106] In another case, the Gujarat High Court held that "The provision is not available to an applicant to make a fishing or roving inquiry"[107]

Order XVI of the CPC lays down the rules to be observed in summoning *witnesses* to give evidence or produce documents. A witness may be summoned to produce documents on a application by a party or on the court's own motion. If a person to whom such a summons has been issued fails, without lawful excuse, to produce the document summoned and the Court "sees reason to believe that such evidence or production is material" it may issue a warrant, either with or without bail, for the arrest of such person, and may make an order for the attachment of his property to such amount as it thinks fit.

Section 162 of the Evidence Act provides that "a witness summoned to produce a document shall, if it is in his possession or power, bring it to the Court, notwithstanding any objection which there may be to its production or to its admissibility. The validity of any such objection shall be decided on by the Court." In *State Of Punjab v Sodhi Sukhdev Singh*, the Supreme Court held that "The provisions of Order XI of the Code of Civil Procedure must be read subject to s. 162 of the Indian Evidence Act and where a privilege is claimed at the stage of inspection, the Court is precluded from inspecting the privileged document in view of s. 162 of the Act."[108]

## 7.2 Production of documents in Criminal cases

Section 91 of the CrPC empowers courts or police officers to requisition, by written order, the production of documents that are "necessary or desirable" for the purpose of "any investigation, inquiry, trial".

---

[106] Sasanagouda v Dr. S.B. Amarkhed And Others, AIR 1992 SC 1163 (1992), http://indiankanoon.org/doc/1169196/ (last visited Oct 9, 2011).

[107] Mr. Pushkar Navnitlal Shah v Mrs. Rakhi Pushkar Shah, AIR 2007 Guj 5 (2006), http://indiankanoon.org/doc/412225/ (last visited Oct 9, 2011).

[108] The State Of Punjab v Sodhi Sukhdev Singh, AIR 1961 SC 493 (1960), http://www.indiankanoon.org/doc/1910029/ (last visited Oct 9, 2011).

This section however limits the application of this power by exempting any "letter, postcard, telegram, or other document or any parcel or thing in the custody of the postal or telegraph authority." Such documents can only be obtained under judicial scrutiny by following a more rigorous procedure laid down in Section 92. Under this latter section, it is only a "District Magistrate, Chief Judicial Magistrate, Court of Session or High Court" who can order the production of documents "in the custody of a postal or telegraph authority " if she determines that it is "wanted for the purpose of any investigation, inquiry, trial". However subordinate courts and officers, such as "any other Magistrate, whether Executive or Judicial, or of any Commissioner of Police or District Superintendent of Police" can require the postal or telegraph authority to search for, and detain such documents in their custody pending the order of a higher court. [Section 92(2) CrPC].

If a Court "has reason to believe"[109] that a person to whom a summons to produce documents has been or would be issued, would not produce the document, it may issue a search warrant against such a person. However only a District Magistrate or Chief Judicial Magistrate may issue a warrant with respect to anything in the custody of the postal or telegraph authority.[110] [Section 93 CrPC]

Section 175 of the Indian Penal Code makes it an offence for a person to "intentionally omit to produce a document which he is legally bound to produce". In case the document was to be delivered to a public servant or police officer, such omission is punishable with simple imprisonment of up to one month, or with fine up to five hundred rupees or both. If the document was to be delivered to a Court of Justice, omission could invite simple imprisonment up to six with or without a fine of one thousand rupees.

[109] There have been a number of decisions by various High Courts and the Supreme Court on the meaning of the expression "reason to believe". In most of these cases, the court has held that the expression requires more than the mere 'subjective satisfaction' of the judge or officer issuing the search order. Thus, for instance, in *Melicio Fernandes v. Mohan* (AIR 1966 Goa 23), the Bombay High Court at Goa held that the expression "contemplates an objective determination based on intelligent care and deliberation involving judicial review, as distinguished from purely subjective consideration"

[110] If a court inferior to these courts issues such a search-warrant, the entire proceedings would be void under Section 461 of the CrPC.

## 7.3 What documents cannot be compelled to be produced?

### 7.3.1 Privileged Communication

The Indian Evidence Act exempts certain witnesses from disclosing documents to Courts. These 'privileges' apply irrespective of whether the proceedings are civil or criminal in nature.

Section 122 of the Evidence Act provides that married couples shall not be compelled or permitted to disclose any communications made *between them* during marriage without the consent of the person who made the communication. 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."

Similarly Section 126 forbids "barristers, attorneys, pleaders or vakils" from disclosing, without their client's express consent, the contents of a) any communication made to them b) any document with which they have become acquainted or c) any advice tendered by them to the client if such information was received by them "in the course and for the purpose of" their 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"

As with the matrimonial privilege, the attorney-client 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,
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 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.

Section 123 of Evidence Act declares that "No one shall be permitted to give any evidence derived from unpublished official records relating to any affairs of State, except with the permission of the officer at the head of the department concerned, who shall give or withhold such permission as he thinks fit." Despite many rulings on the subject, it is still unclear how wide or narrow the ambit of "affairs of state" is. Does it include everything that the state does so that all records maintained by the state pertain to affairs of the state, or, does it only pertain to those confidential matters, disclosure of which would be detrimental to public interest, national defence or good diplomatic relations? Specifically, for instance, if the government maintains routine records about individuals in the course of governance, would these count as "official records relating to affairs of state"? In a few pre-independence cases, it was held that records of income tax returns submitted to income tax officials were not "affairs of state" and hence no privilege could be claimed with respect to them.[111] Although subsequent amendments to the Income Tax Act conferred confidentiality on these records, in an era when the government has begun to maintain minute records of every aspect of citizens' lives, it still begs the question on what kind of documents may be declared privileged.

Section 124 similarly shields public officers from being compelled to disclose communications made to them in official confidence, when the public interest would suffer by the disclosure.

Section 130 exempts witnesses who are not a party to a suit from being compelled to produce their "title-deeds to any property, or any document in virtue of which he holds any property as pledgee or mortgagee, or any document the production of which might tend to criminate him, unless he has agreed in writing to produce them with the person seeking the production of such deeds or some person through whom he claims"

[111] Venkatachella v. Sampatu Chettiar (1909) ILR 32, Jadabaram v. Bulloram (1899) ILR 26 Cal 281

As noted previously, in all the aforementioned situations Section 162 of the Evidence Act provides that the witness must bring the document to court and then state his objections to the Court.

### 7.3.2 Self Incriminating Documents

Article 20(3) of the Indian Constitution enacts a rule against self-incrimination and provides that "No person accused of any offence shall be compelled to be a witness against himself". This operates as an additional threshold limit on the power of criminal courts to order the production of documents. In a very early case, the Supreme Court held that "compelled production of incriminating documents by an accused person.. is testimonial compulsion within the meaning of art. 20(3) of the Constitution."[112] Accordingly the court held that it was impermissible to issue summons for the production of documents under Sections 91 and 92 of the CrPC. However, the Court went on to hold that "a search and seizure of a document under the provisions of [Section 93] of the Code of Criminal Procedure is not a compelled production thereof within the meaning of art. 20 (3) and hence does not offend the said Article." In other words, although a criminal court cannot summon an accused to produce an incriminating document, the court may order instead, his house to be searched in order to retrieve the same document.

In *State Of Maharashtra v The Nagpur Electric Light Company*[113], the Supreme Court held that summons could not be issued to the Store Keeper and Assistant Accountant of a company to produce documents that would incriminate the company since even incorporated entities were 'persons' who were entitled to the protection of Article 20(3).

- what legal regimes govern how law enforcement agencies gain access to personal information held by individuals and organisations?

- were extraneous powers introduced to deal with national security and counter-terrorism? how are these implemented and reported upon?

[112] M. P. Sharma v Satish Chandra, AIR 1954 SC 300 (1954), http://indiankanoon.org/doc/1306519/ (last visited Oct 9, 2011).
[113] 1961 CriLJ 200

- what happens in circumstances where requests come from foreign governments, or where the government has to request information from other countries? e.g. Google Transparency report, bilateral and multi-lateral conventions

## §8 Intelligence and Surveillance Oversight

Under the Constitution, 'Public Order' and 'Police' are subjects on which the States have exclusive jurisdiction to legislate. Accordingly each state maintains its own separate police force under a state-specific Police Act, and this force is responsible for maintenance of law and order and gathering local intelligence within the territory of that state. However, the Union Government is given exclusive powers to legislate on the subject of "Central Bureau of Intelligence and Investigation."

The Central Bureau of Investigation is the Central Government's primary investigative agency. Although created by enactment in 1946 as the Delhi Special Police Establishment (SPE) to investigate cases of bribery and corruption by Central Government employees, over the years its jurisdiction was expanded to include a range of "Economic Offences and important conventional crimes such as murders, kidnapping, terrorist crimes, etc"[114] Due to the federal setup of police powers in India, the CBI can take up cases within the boundaries of a State only with the prior consent of that State. Today, the CBI carries out its functions under three main divisions: (i) Anti-Corruption Division - for investigation of cases under the Prevention of Corruption Act, 1988 against Public officials and the employees of Central Government, Public Sector Undertakings (ii) Economic Offences Division - for investigation of major financial scams and serious economic frauds, including crimes relating to Fake Indian Currency Notes, Bank Frauds and Cyber Crime (iii) Special Crimes Division - for investigation of serious, sensational and organized crime under the Indian Penal Code and other laws on the requests of State Governments or on the orders of the Supreme Court and High Courts. In addition, the CBI is designated as the National Crime Bureau – India Interpol since 1966. It is the only agency

[114] A Brief History of CBI, CENTRAL BUREAU OF INVESTIGATION, http://cbi.nic.in/history.php (last visited Oct 9, 2011).

recognized by Interpol Secretariat General for bilateral as well as multilateral police co-operation among member states.[115]

In 2007, a Parliamentary Committee proposed the reconstitution of the CBI as the "Central Bureau of Intelligence and Investigation" to empower it to gather intelligence and fulfill its Constitutional mandate.[116]

In 2008, a new statutory body called the National Investigation Agency was created specifically to combat terrorist threats and address the shortcomings of the CBI. Set up in the aftermath of the tragic Mumbai Terror Attacks in November 2008, the NIA was tasked with the mandate to "investigate and prosecute offences affecting the sovereignty, security and integrity of India, friendly relations with foreign States and offences under Acts enacted to implement international treaties, agreements, conventions and resolutions of the United Nations and other international organizations and for matters connected therewith or incidental thereto."

## §9 Immigration and Privacy

Like most countries in the world, India requires foreigners to obtain a visa before entering the country. Standard documentation is required to obtain a visa including proof of address, passport photographs and invitation letters.

The presence of foreigners in India is regulated by the provisions and rules under the Foreigners Act 1946 and the Registration of Foreigners Act 1939.

Foreigners visiting India on long term visas (more than 180 days) are required to get themselves registered with concerned Foreigners Regional Registration Officers (FRROs) within 14 days of their first arrival. The District Superintendents of Police typically function as Foreigners Registration Officers in each State. The process of registration entails the submission of a number of records, passport size photographs etc. Although foreigners are not currently required to submit biometric details, this is a plan that is being developed. Under the 'Immigration, Visa and Foreigners Registration & Tracking (IVFRT)' system, under the National E-Governance

115

116 Par Panel favours reconstituting of CBI as CBII, ECONOMIC TIMES, December 23, 2007, http://articles.economictimes.indiatimes.com/2007-12-23/news/27673939_1_terror-attacks-intelligence-agencies-central-bureau (last visited Oct 9, 2011).

Plan, the Ministry of Home Affairs aims to "enable authentication of traveler's identity at the Missions, Immigration Check Posts (ICPs) and Foreigners Registration Offices (FROs) through use of intelligent document scanners and biometrics, updation of foreigner's details at entry and exit points, improved tracking of foreigner's through sharing of information captured during visa issuance at Missions, during immigration check at ICPs, and during registration at FRRO/ FROs"[117] The scope of the project includes 169 Missions, 77 ICPs (Immigration Check Posts), 5 FRROs (Foreigners Regional Registration Offices), and FROs (Foreigners Registration Offices) in the State/District Headquarters.[118]

Once registered, a foreigner may be compelled to produce sets of finger impressions, passport photographs and signatures if the proof of identity submitted by him during registration does not contain these details.[119]

Apart from this, "Every keeper of a hotel" is required to maintain a separate Register for foreigners. They are required to transmit within twenty four hours after the arrival of any foreigner, a copy of a memo containing details about the foreigner to the Registration Officer.

## §10 Travel and Borders

An immigration check is carried out for all passengers at the port of arrival in India by the Bureau of Immigration. Passengers (both Indian and foreign) entering the country are required to furnish details about themselves in the disembarkation card( Arrival Card) including their name and nationality, age, sex, place of birth and address or intended address in India, the purpose of visit and the proposed length of stay in India. Immigration check includes "checking of Passport, Visa, Disembarkation Card, entering foreigner's particulars in computer, retention of Arrival Card and stamping of passport of the foreigner".[120]

---

[117] Immigration, Visa and Foreigner's Registration & Tracking (IVFRT), Government of India, Department of Information Technology (DIT) (2010), http://www.mit.gov.in/content/ivfrt (last visited Oct 9, 2011).; Sahil Makkar & Surabhi Agarwal, Biometric-based identification for foreign workers may be introduced, LIVEMINT, July 19, 2010, http://www.livemint.com/2010/07/19234500/Biometricbased-identification.html (last visited Oct 9, 2011).

[118] *Ibid*

[119] *General Requirements For Registration Of A Foreign National*, BUREAU OF IMMIGRATION, MINISTRY OF HOME AFFAIRS, http://www.immigrationinhttp://www.immigrationindia.nic.in/reg_req2.htm#lprc101dia.nic.in/Instr_foreigners2.htm (last visited Oct 9, 2011).

[120] Instruction For Foreigners Coming To India, BUREAU OF IMMIGRATION, http://www.immigrationindia.nic.in/Instr_foreigners2.htm (last visited Oct 9, 2011).

Customs rules permit passengers to bring up to two laptops into the country without paying additional duty. Customs officials are empowered to seize laptops that are sought to be smuggled into India over and above this permissible quota.

There have been no reported cases of Customs or immigration officials having searched laptops at the borders in India.

## §11 Profiling/Data Mining

There are currently no laws in India that specifically either proscribe or permit profiling or data mining in a general way. Article 14 of the Constitution of India grants all citizens the right to 'equality and equal protection' and to the extent that the state conducts profiling to the disadvantage of any citizen or class of citizens, this article may be viewed as a 'law against profiling'.

## §12 DNA and other Forensic tests to determine identity

India does not currently have a national DNA database, although there is a bill pending in Parliament that envisages the creation of such a database. The draft DNA Profiling Bill, pending since 2007 before Parliament, attempts to create a centralized DNA bank that would store DNA records of virtually anyone who comes within any proximity to the criminal justice system. Specifically, records are to be maintained of "suspects, offenders, missing persons and 'volunteers'".[121] 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.[122]

Meanwhile the infrastructure for DNA testing by both State and private players to create such databases has proliferated. In June 2008, newspapers reported that a 'Biotech Park' in Lucknow in the north India had announced the setting up of a DNA Bank – purportedly Asia's first. "The

[121] The Bill provides for the following indices to be maintained : (i) a crime-scene index; (ii) a suspects' index; (iii) an offenders' index; (iv) a missing persons' index; (v) unknown deceased persons' index; (vi) a volunteers' index; (vii) such other indices as may be specified by regulations.
[122] Draft DNA Profiling Bill, , http://dbtindia.nic.in/DNA_Bill.pdf (last visited Sep 26, 2011).

members of the DNA bank will receive a microchip based DNA card containing information of their fingerprints, and anthropological details, said Seth", the report said.[123]
In December 2010, Nehru Nagar, a region in Mumbai announced that it had established a DNA database of over 800 "anti-social elements and other people from the area".[124]

In January 2011, the Indian Army began DNA profiling of its soldiers in order to "to help in identification of bodies mutilated beyond recognition."[125]

Even without the DNA Profiling bill, various existing laws already permit the collection of a range of physiological evidence.
The pre-independence Identification Of Prisoners Act, 1920 empowers police officers to take "measurements" (including finger-impressions and foot-print impressions) and photographs 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.[126] 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.[127]
The Act also provides for the destruction of all photographs and records of measurements on discharge or acquittal.[128]
In 2005, the Code of Criminal Procedure was amended to enable the collection of a host of medical details from accused persons upon their arrest. Section 53 of the CrPC 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

[123] Asia's first human DNA bank comes up in Lucknow, DNA INDIA, June 11, 2008, http://www.dnaindia.com/india/report_asia-s-first-human-dna-bank-comes-up-in-lucknow_1170426 (last visited Sep 26, 2011).
[124] Shankar Abidi, *Nehru Nagar first region in country to have DNA profiling database - Mumbai*, DNA INDIA, December 6, 2010, http://www.dnaindia.com/mumbai/report_nehru-nagar-first-region-in-country-to-have-dna-profiling-database_1477211 (last visited Sep 26, 2011).
[125] DNA profiling of army personnel to begin soon, DNA India, January 2, 2011, http://www.dnaindia.com/india/report_dna-profiling-of-army-personnel-to-begin-soon_1489153 (last visited Sep 26, 2011).
[126] Sections 3 & 4 of the Identification Of Prisoners Act, 1920
[127] Ibid, Section 5
[128] Section 7

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[129] affirmed the legality of ordering a DNA test in criminal cases to ascertain the involvement of persons accused. Refusal to co-operate 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"[130]

It is evident that the utility of this mass of information – fingerprints, handwriting samples and photographs, DNA data – in solving crimes is immense. Without having said 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 vs Kathi Kalu Oghad And Others*[131] The petitioner contended that the obtaining of evidence through legislations such as the Identification of

---

[129] *Thogorani Alias K. Damayanti vs State Of Orissa And Ors* 2004 Cri L J 4003 (Ori) < http://indiankanoon.org/doc/860378/>

[130] *Ibid*

[131] AIR 1961 SC 1808 < http://indiankanoon.org/doc/1626264/>

Prisoners Act amounted to compelling the person accused of an offence "to be a witness against himself" in contravention of Art. 20(3) of the Constitution. The court held that "there was no infringement of Art. 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*."[132]

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 'exorcise' truth and lies directly from their body. One statement by Dr M.S. Rao, Chief Forensic Scientist, Government of India captures this shift:

> 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.[133]

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"[134]

---

[132] *Ibid*
[133] Keynote address given to the 93rd Indian Science Congress. See http://mindjustice.org/india2-06.htm, cited in Liang, L., 2007. And nothing but the truth, so help me science. In *Sarai Reader 07 - Frontiers*. Delhi: CSDS, Delhi, pp. 100-110. Available at: http://www.sarai.net/publications/readers/07-frontiers/100-110_lawrence.pdf [Accessed April 11, 2011].
[134] *Ibid*

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."[135]

This position was however overturned recently by the Supreme Court in *Selvi v. State of Karnataka*[136] (2010). 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 thoroughgoing 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*

[135] Ramchandra Ram Reddy v. State of Maharashtra [1 (2205) CCR 355 (DB)
[136] (2010) 7 SCC 263 http://indiankanoon.org/doc/338008/

*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. 250
>
> (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.

## §13 Communications Surveillance and Data Retention

This section provides a brief overview of the provisions in various Indian laws that delimit the powers of the State to intercept communications.

In general, all communications are presumed to be entitled to privacy. Thus all laws in India dealing with mediums of inter-personal communication – post, telegraph and telephony and email – contain sections prohibiting the unlawful interception of communication.[137]

However, each of these laws also contain analogously worded provisions permitting interception by the State under specified conditions.

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 tranquility". 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 tranquility.

Similarly, Section 5(2) of the Telegraph Act 1885 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) defense of India,

[137] Thus, for instance, Sections 24 and 25 of the Telegraph Act 1885 penalize acts of persons that are intended to "learn the contents of messages" or "to intercept or to acquaint himself with the contents of any message" or "prevent or obstruct the transmission or delivery of any message. Similarly, the Post Office Act of 1898 contains a range of offences which penalise the detention, altering, diversion of letters/post office articles.

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 bare 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' to do so.

In *Hukam Chand Shyam Lal v. Union Of India and ors*[138], 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

[138] AIR 1976 SC 789 , 1976 SCR (2)1060 , (1976) 2 SCC 128

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.”[139]

Another, relatively more recent elaboration of these terms occurs in the case of *PUCL v. Union of India*[140]. Here the Court observed:

> "Public emergency would mean the prevailing of a sudden condition or state of affairs affecting the people at large calling for immediate action. The expression "public safety" means the state or condition of freedom from danger or risk for the people at large, When either of these two conditions are not in existence, the Central Government or a State Government or the authorised officer cannot resort to telephone tapping even though there is satisfaction that it is necessary or expedient so to do in the interests of it sovereignty and integrity of India etc. *In other words, even if the Central Government is satisfied that it is necessary or expedient so to do in the interest of the sovereignty and integrity of India or the security of the State or friendly relations with sovereign States or in public order or for preventing incitement to the commission of an offence, it cannot intercept the message, or resort to telephone tapping unless a public emergency has occurred or the interest of public safety or the existence of the interest of public safety requires.* Neither the occurrence of public emergency nor the interest of public safety are secretive conditions or situations. *Either of the situations would be apparent to a reasonable person*.” (emphasis added)

Thus the phrases ‘public emergency’ and ‘public safety’ do 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

[139] Romesh Thappar vs The State Of Madras AIR 1950 SC 124 , 1950 SCR 594
[140] AIR 1997 SC 568

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". Paradoxically, it would appear from the foregoing discussion, that the two colonial legislations are more attentive to the safeguarding of privacy than the more post-independence one. In the next sub-sections, we take a closer look at the separate surveillance and interception regimes under the Telegraph Act (governing most telephony) and the Information Technology Act (governing most electronic communications)

## 13.1 Wiretapping under the Telegraph Act

In February 2011, Reliance Communications, a large telecom service provider disclosed to the Supreme Court that over a hundred and fifty thousand telephones had been tapped by it between 2006 and 2010 – almost 30,000 a year. A majority of these interceptions were conducted based on orders issued from state police departments whose legal authority to issue them is suspect. New rules framed under the Telegraph Act in 2007 required such orders to be issued only by a high-ranking Secretary in the Department/Ministry of Home Affairs.[141] In this section we look at the regime of interception under the Telegraph Act and licenses issued under it.

First enacted in 1885, the Telegraph Act remains today on the statute books as the umbrella legislation governing most forms of electronic communications in India including telephones, faxes, the internet etc.. The Act contains several provisions which regulate and prohibit the unauthorized interception or tampering with messages sent over 'telegraphs'[142]. The following sections apply:

1) Section 5 empowers the Government to take possession of licensed telegraphs and to order interception of messages in cases of 'public emergency' or 'in the interest of the

[141] *Telegraph (Amendment) Rules 2007*, Available at: http://www.dot.gov.in/Acts/English.pdf [Accessed June 28, 2011].

[142] 'Telegraph' is defined widely in the Act to include any "apparatus used or capable of use for transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature" thus covering most known mediums of communication.

public safety'. Interception may only be carried out pursuant to a written order by an officer specifically empowered for this purpose by the State/Central Government. The officer must be 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"[143]

2) Section 23 imposes a fine of Rs. 500 on anyone who enters a telegraph office without proper authorization.

3) Section 24 makes it a criminal offence for a person to enter a telegraph office "with the intent of unlawfully learning the contents of any message". Such a person may be punished with imprisonment for a term of up to a year.

4) Section 25 further imposes a criminal penalty on anyone who damages or tampers with any telegraph with the intent to prevent the transmission of messages or to acquaint himself with the contents of any message or to commit mischief. Punishment in this case could extend to 3 years imprisonment or a fine or both.

5) Section 26 makes it an offence for a Telegraph Officer to alter, unlawfully disclose or acquaint himself with the content of any message. This is also punishable with up to 3 years imprisonment or a fine or both.

6) Section 30 criminalizes the fraudulent retention or willful detention of a message which is intended for someone else. Punishment extends to 2 years imprisonment or fine or both.

Although the statutory provisions themselves govern the actions of telecom operators in a general way, more detailed guidelines regulating their behavior are contained in the terms of the

[143] In 1997, the Supreme Court of India held in *PUCL v. Union of India* that the interception of communications under this section was unlawful unless carried out according to procedure established by law. Since no Rules had been prescribed by the Government specifying the procedure to be followed, the Supreme Court framed guidelines to be followed before tapping of telephonic conversation. These guidelines have been substantially incorporated into the Indian Telegraph Rules in 2007. Rule 419A 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.

*licenses* issued to them which permit them to conduct business[144]. Frequently these licenses contain clauses requiring telecom operators to safeguard the privacy of their consumers. A few examples would suffice here:

### 13.1.1 National Long Distance License

1) Clause 21 of the National Long Distance License[145] comprehensively covers various aspects of privacy including

    a. Licensees to be responsible for the protection of privacy of communication, and to ensure that unauthorised interception of message does not take place.

    b. Licensees to take all necessary steps to safeguard the privacy and confidentiality of any information about a third party and their business to whom they provide service and from whom they have acquired such information by virtue of those service and shall use their best endeavours to secure that :

        i. No person acting on behalf of the Licensees or the Licensees themselves divulge or uses any such information except as may be necessary in the course of providing such service to the Third Party; and

        ii. No such person seeks such information other than is necessary for the purpose of providing service to the Third Party.

    c. The above safeguard however does not apply where

        i. The information relates to a specific party and that party has consented in writing to such information being divulged or used, and such information is divulged or used in accordance with the terms of that consent; or

        ii. The information is already open to the public and otherwise known.

    d. The Licensees shall take necessary steps to ensure that the they and any person(s) acting on their behalf observe confidentiality of customer information..

[144] Section 4 of the Telegraph Act forbids the establishment of any telegraph service (including, as mentioned earlier, all telephony, internet etc) without obtaining a license from the Central Government.
[145] Issued to TSPs who offer long distance telephony in India

### 13.1.2 Unified Access Service License/ Cellular Mobile Telephone Service License

Clause 39.2 of the Unified Access Service License and clause 42.2 of the Cellular Mobile Telephone Service license enjoin the licensee to take all necessary steps to safeguard the privacy and confidentiality of any information about a third party and its business to whom it provides the service. The Licensee is required to use its best endeavors to secure that no person acting on behalf of the licensee or the licensee divulges or uses any such information except as may be necessary in the course of providing such service to the third party.

### 13.1.3 Monitoring of internet users under the ISP licenses

The Internet Services License Agreement (which authorizes ISPs to function in India) contains provisions requiring telecom operators to safeguard the privacy of their consumers or to co-operate with government agencies when required to do so. Some of the important clauses in this agreement are:

a) Part VI of the License Agreement gives the Government the right to inspect/monitor the ISPs systems. The ISP is responsible for making facilities available for such interception.

b) Clause 32 under Part VI contains provisions mandating the confidentiality of information held by ISPs. These provisions hold ISPs responsible for the protection of privacy of communication, and to ensure that unauthorised interception of message does not take place. Towards this, ISPs are required:

    a. to take all necessary steps to safeguard the privacy and confidentiality of any information about a third party and their business to whom they provide service and from whom they have acquired such information by virtue of those service and shall use their best endeavours to secure that :

    b. to ensure that no person acting on behalf of the ISPs divulge or uses any such information except as may be necessary in the course of providing such service to the Third Party; and

    c. This safeguard however does not apply where

        i. The information relates to a specific party and that party has consented in writing to such information being divulged or used, and such information is divulged or used in accordance with the terms of that consent; or

        ii. The information is already open to the public and otherwise known.

d. To take necessary steps to ensure that any person(s) acting on their behalf observe confidentiality of customer information.

c) Clause 33.4 makes it the responsibility of the ISP to trace nuisance, obnoxious or malicious calls, messages or communications transported through its equipment.

d) Clause 34.8 requires ISPs to maintain a log of all users connected and the service they are using (mail, telnet, http etc.). The ISPs must also log every outward login or telnet through their computers. These logs, as well as copies of all the packets originating from the Customer Premises Equipment (CPE) of the ISP, must be available in REAL TIME to Telecom Authority. The Clause forbids logins where the identity of the logged-in user is not known.

e) Clause 34.12 and 34.13 requires the ISP to make available a list of all subscribers to its services on a password protected website for easy access by Government authorities.

f) Clause 34.16 requires the ISP to activate services only after verifying the bonafides of the subscribers and collecting supporting documentation. There is no regulation governing how long this information is to be retained.

g) Clause 34.22 makes it mandatory for the Licensee to make available "details of the subscribers using the service" to the Government or its representatives "at any prescribed instant".

h) Clause 34.23 mandates that the ISP maintain "all commercial records with regard to the communications exchanged on the network" for a period of "at least one year for scrutiny by the Licensor for security reasons and may be destroyed thereafter unless directed otherwise by the licensor".

i) Clause 34.28 (viii) forbids the ISP from transferring the following information to any person/place outside India:

   a. Any accounting information relating to subscriber (except for international roaming/billing) (Note: it does not restrict a statutorily required disclosure of financial nature) ; and

   b. User information (except pertaining to foreign subscribers using Indian Operator's network while roaming).

j) Clause 34.28(ix) and (x) require the ISP to provide traceable identity of their subscribers and on request by the Government must be able to provide the geographical location of any subscriber at any given time.

k) Clause 34.28(xix) stipulates that "in order to maintain the privacy of voice and data, *monitoring shall only be upon authorisation by the Union Home Secretary or Home Secretaries of the States/Union Territories*". (It is unclear whether this is to operate as an overriding provision governing all other clauses as well)

From the list above, it is very clear that by the terms of their licenses, ISPs are required to maintain extensive logs of user activity for unspecified periods. However, it is unclear, in practice, to what extent these requirements are being followed by ISPs. For instance, an article in the Economic Times in December 2010[146] reports:

> "The Intelligence Bureau wants internet service providers, or ISPs, to keep a record of all online activities of customers for a minimum of six months
>
> *Currently, mobile phone companies and internet service providers do not keep online logs that track the web usage pattern of their customers. They selectively monitor online activities of only those customers as required by intelligence and security agencies, explained an executive with a telecom company.*" (emphasis added)

The same news report quotes Rajesh Chharia, President of the Internet Service Providers' Association of India,.as saying "At present, we only keep a log of all our customers' Internet Protocol address, which is the digital address of a customer's internet connection."

The news report goes on to disclose the ambitious plans of the Intelligence Bureau to "put in place a system that can uniquely identify any person using the internet across the country" through "a technology platform where users will have to mandatorily submit some form of an online identification or password to access the internet every time they go online, irrespective of the service provider." Worryingly, the report goes on to discuss the setting up by the telecommunications department of "India's indigenously-built Centralised Monitoring System

[146] Thomas Philip, J., 2010. Intelligence Bureau wants ISPs to log all customer details. *Economic Times*. Available at: http://articles.economictimes.indiatimes.com/2010-12-30/news/27621627_1_online-privacy-internet-protocol-isps [Accessed June 28, 2011].

(CMS), which can track all communication traffic—wireless and fixed line, satellite, internet, e-mails and voice over internet protocol (VoIP) calls—and gather intelligence inputs. The centralised system, modeled on similar set-ups in several Western countries, aims to be a one-stop solution as against the current practice of running several decentralised monitoring agencies under various ministries, where each one has contrasting processing systems, technology platforms and clearance levels." Although as of this writing, this CMS is not yet fully functional, it's launch seems to be imminent and will inaugurate with it, an era of constant and continuous surveillance of all internet users.

## 13.2 Interception of Electronic Communications under the Information Technology Act

There are two regimes of interception and monitoring information under separate sections the Information Technology Act. Both would seem capable of authorising access of IP Addresses, among other information to government agencies.

Section 69 deals with "Power to issue directions for interception or monitoring or decryption of any information through any computer resource". In addition, the Government has been given a more generalised monitoring power under Section 69B to "monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource". This monitoring power may be used to aid a range of "purposes related to cyber security"[147]. "Traffic data" has been defined in the section to mean "any data identifying or purporting to identify any person, computer system or computer network or any location to or from which communication is or may be transmitted."

Rules have been issued by the Central Government under both these sections[148] which are similar, although with important distinctions. These rules stipulate the manner in which the

[147] The Monitoring Rules list 10 'cyber security' concerns for which Monitoring may be ordered: (a) forecasting of imminent cyber incidents; (b) monitoring network application with traffic data or information on computer resource; (c) identification and determination of viruses/computer contaminant; (d) tracking cyber security breaches or cyber security incidents; (e) tracking computer resource breaching cyber security or spreading virus/computer contaminants; (f) identifying or tracking of any person who has contravened, or is suspected of having contravened or being likely to contravene cyber security; (g) undertaking forensic of the concerned computer resource as a part of investigation or internal audit of information security practices in the computer resource;(h) accessing a stored information for enforcement of any provisions of the laws relating to cyber security for the time being in force; (i) any other matter relating to cyber security.

[148] Respectively the INFORMATION TECHNOLOGY (PROCEDURE AND SAFEGUARDS FOR INTERCEPTION, MONITORING AND DECRYPTION OF INFORMATION) RULES, 2009, G.S.R. 780(E) (2009),

powers conferred by the sections may be exercised. The rules framed under Section 69 and Section 69B contain important safeguards stipulating, *inter alia*, to a) Who may issue directions of interception and monitoring b) How are the directions to be executed c) The duration they remain in operation d) to whom data may be disclosed e) Confidentiality obligations of intermediaries f) Periodic oversight of interception directions by a Review Committee under the Telegraph Act g)maintenance of records of interception by intermediaries h) Mandatory destruction of information in appropriate cases.

The important difference between the two sections is that while Section 69 provides a mechanism whereby specific computer resources can be monitored in order to learn the contents of communications that pass through such resource, Section 69B by contrast provides a mechanism for obtaining 'meta-data' about all communications transacted using a computer resource over a period of time – their sources, destinations, routes, duration, time etc without actually learning the content of the messages involved. The latter type of monitoring is specifically in order to combat threats to 'cyber security', while the former can be invoked for a number of purposes such as the securing of public order and criminal investigation[149].

However, this distinction is not very sharp – an interception order under Section 69 directed at a computer resource located in an ISP can yield traffic data in addition to the content of all communications. Thus for instance, if a direction was passed ordering my ISP to intercept "all communications sent or received by Prashant Iyengar", the information obtained by such interception would include a resume of all emails exchanged, websites visited, files downloaded etc. In such a case, a separate order under Section 69B would be unnecessary. An important clue about their relative importance may lie in the different purposes for which each section may be invoked coupled with the fact that while directions under Section 69 can be issued by officers both at the central and state level, directions under Section 69B can only be issued by the Secretary of the Department of Information Technology under the Union Ministry of

---

http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/Itrules301009.pdf (last visited Jun 30, 2011). and INFORMATION TECHNOLOGY (PROCEDURE AND SAFEGUARDS FOR MONITORING AND COLLECTING TRAFFIC DATA OR INFORMATION) RULES, 2009, G.S.R. 782(E) (2009), http://cca.gov.in/rw/resource/gsr782.pdf?download=true (last visited Jun 30, 2011).

[149] Section 69 lists the following grounds for which interception may be ordered : a) sovereignty or integrity of India, b) defense 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,

Communications and Information Technology. [150] This indicates that the collection of traffic data by the government under Section 69B is intended to facilitate the securing of India's 'cyber security' from possible *external* threats – a Defence function – while the interception powers under Section 69 are to be exercised for more domestic purposes as aids to Police functions.

Although these sections provide powerful tools of surveillance in the hands of the state, these powers may only be exercised by observing the rather tedious procedures laid down. In the absence of any systematic data on interception orders, it is unclear to what extent these powers are in fact being used in the manner laid down.

- how many requests are there per year for interception of content? how many requests for traffic data? is there any certainty that all communications surveillance operates under the rule of law?

## 13.3 Data Retention Requirements

Section 67C of the IT Act requires 'intermediaries' to maintain and preserve certain information under their control for durations. Both the categories of information and the duration of their retention are to be specified in rules to be notified by the Central Government. Failure by an intermediary to retain such electronic records is punishable with imprisonment up to three years and a fine [Sec 67C(2)].

As of this writing, (except in relation to cyber cafes, discussed later in this document) no rules have been framed under this section which specify the kinds of information and the duration for which such information must be retained by intermediaries.

An 'Intermediary' has been defined very expansively under section 2(w) of the Act to mean, with respect to any electronic record, "any person who on behalf of another person receives, stores or transmits that record, or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, webhosting service providers, search engines, online payment sites, online-auction sites, online-market

[150] Rule 2(d) of the Monitoring and Collecting of Traffic Data Rules 2009

places and cyber cafes". It is evident, on a plain reading, that this definition includes virtually any node through which 'electronic records'[151] may be transferred.

The pre-independence Destruction of Records Act, 1917 empowers the appropriate Government – Central or State – to determine the schedule for destruction of records with respect to all public authorities within their purview. It also empowers the High Court to determine the retention schedule for all courts subordinate to it. Rules framed under the Act provide for destruction of records by various functionaries including, for instance, the bodies under the Companies Act including the Registrar of Companies[152], the Company Law Board[153] and the Office of the Public Trustee.[154]

Several government organisations have their own internal "destruction schedule". For instance, the Central Vigilance Commission has an elaborate schedule of shredding according to which the organisation shreds some of its data periodically, while retaining other data permanently.[155]

In addition several statutory instruments contain data retention provisions appropriate to their context – for instance, Rule 33 of the Registration of Electors Rules, 1960 requires all records relating to the preparation of electoral rolls to be kept by the registration officer for a period of a year following the publication of the rolls. These records must be shredded upon the completion of that period.[156]

---

[151] "electronic record" under the Information Technology Act means "data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche"

[152] DISPOSAL OF RECORDS (IN THE OFFICES OF THE REGISTRARS OF COMPANIES) RULES, 2003 (2003), http://www.mca.gov.in/Ministry/actsbills/rules/DoRitOotRoCR2003.pdf (last visited Oct 31, 2011).

[153] THE OFFICES OF THE COMPANY LAW BOARD BENCHES (DESTRUCTION OF RECORDS) RULES, 1980, http://www.mca.gov.in/Ministry/actsbills/rules/TOOTCLBBDORR1980.pdf (last visited Oct 31, 2011).

[154] THE OFFICE OF THE PUBLIC TRUSTEE (DESTRUCTION OF RECORDS) RULES 1984 (1984), http://www.mca.gov.in/Ministry/actsbills/rules/TOOTPTDoRR1984.pdf (last visited Oct 31, 2011).

[155] RETENTION PERIOD/DESTRUCTION SCHEDULE OF RECORDED FILES. (2006), http://cvc.nic.in/retention.pdf (last visited Oct 31, 2011).

[156] Hand Book for Electoral Registration Officers Election Commission of India 2008, 57 (2008), http://eci.nic.in/eci_main/ElectoralLaws/HandBooks/ERO_HANDBOOK.pdf (last visited Oct 30, 2011); REGISTRATION OF ELECTOR RULES, 1960, Rule 33 (1961), http://lawmin.nic.in/legislative/election/volume%202/registration%20of%20electors%20rules,%201960.pdf (last visited Oct 30, 2011).

Rule 6F of the Income Tax Rules require specified professionals[157] to preserve their books of accounts for a period of 6 years after the assessment year.[158]

Rules framed under the Companies Act 1956 require all Indian Companies to preserve certain records permanently, and permit other records to be destroyed according to a varying schedule, depending on the type of document, from 8 to 15 years. A record of documents destroyed is also to be maintained under these Rules.[159]

## §14 Visual surveillance

> "According to Frost & Sullivan, the video surveillance market in India grew by 24.5% in 2010 and amassed revenues of $135 mn. IP surveillance systems accounted for almost 28% of the overall value of the surveillance industry." Express Computer[160]

According to a number of market research reports, Asia, and within Asia, India is poised to be one of the biggest markets for surveillance technology in the world. The volatile security environment in the country is one reason many attribute to this growth. As one research report puts it bluntly, "Increasing terrorist activities and attacks have created strong demand for advanced safety and security solutions. As a result, the CCTV market in India is anticipated to grow at a CAGR of more than 30% between 2010 and 2013"[161]

In May 2008, Japan-based CBC Co Ltd – a major manufacturer of CCTVs announced plans to set up a production facility in India through which they hoped to sell "50,000 units of CCTVs every year to be set up across retail malls, real estate projects, industrial houses and government aided infrastructure projects such as subways, highways, heavy traffic zones such as railways stations, airports (Mumbai airport) and huge commercial buildings".[162] This gestures both to the

---

[157] Specifically "Every person carrying on legal, medical, engineering or architectural profession or the profession of accountancy or technical consultancy or interior decoration or authorised representative or film artist" [Rule 6F of the Income Tax Act]

[158] INCOME TAX RULES 1962 6F (1962), http://goo.gl/KSW2S (last visited Oct 31, 2011).

[159] COMPANIES (PRESERVATION AND DISPOSAL OF RECORDS) RULES, 1966 (1966), http://www.mca.gov.in/Ministry/actsbills/rules/CPaDoRR1966.pdf (last visited Oct 31, 2011).

[160] Heena Jhingan, *Under surveillance*, Express Computer, 2011, http://www.expresscomputeronline.com/20110630/securitystrategies01.shtml (last visited Oct 16, 2011).

[161] SECURITY CONCERNS TO DRIVE CCTV DEMAND IN INDIA RNCOS (2010), http://www.rncos.com/Press_Releases/Security-Concerns-to-Drive-CCTV-Demand-in-India.htm (last visited Oct 16, 2011).

[162] Mona Mehta, *Japan's CBC may tap soaring CCTV market*, FINANCIAL EXPRESS, May 19, 2008, http://www.financialexpress.com/news/japans-cbc-may-tap-soaring-cctv-market/311471/ (last visited Oct 17, 2011).

aggressive growth of the market for CCTVs in India, and also indicates the range of potential customers for these products.

Aside from industry reports of these kinds, this growth of CCTV technology is verifiable anecdotally, through media reports and through the quotidian experience of living in any of India's cities and towns. Both the government and private businesses have enthusiastically embraced CCTV technology and they have, in a relatively short time, attained near-ubiquity as municipal corporations, police departments, airports, banks, schools, supermarkets and malls increasingly scramble to install their own private networks of surveillance. A few vignettes of CCTV usage in the country – both by the private sector and the public sector - would illustrate how deeply entrenched the faith in CCTV systems has become:

1. The Delhi International Airport reportedly has the "largest single installation of an IP video system anywhere in Asia" with more than 3700 IP Surveillance cameras piping video feeds into the airport's Operation Control Centre. The OCC reportedly boasts the biggest video wall in Asia. "The 32 x 16 foot wall holds twenty-eight 70-inch screens that display the information inputs from all the airport departments through live camera feeds. Each screen can display up to 25 multiple camera images, providing the AOCC with the capacity to display 700 images at one time." [163] In October 2011, the village of Budania in Rajasthan decided to install twenty CCTVs in their administrative offices and provide live feeds over the internet in a bid to enahance transparency.[164] More than any real assistance to the airport police that such an aggregation of images may provide, or any actual boost in transparency that the CCTV's in Budania might achieve, these two installations are a testament to India's deep enamor of video surveillance technology.
2. The police in a number of Indian cities have issued directions requiring public places such as theatres, hotels, guest-houses, colleges, jewellery shops, cyber cafes, malls and departmental stores to install CCTV cameras. An incomplete inventory of such cities

[163] *IndigoVision deploys huge IP video system at Delhi Airport's Terminal 3*, GOVERNMENT SECURITY NEWS (2011), http://www.gsnmagazine.com/node/22954 (last visited Oct 16, 2011).
[164] Shweta Rao, *Rajasthan Village Uses IT to Fight Corruption*, CIO INDIA NEWS (October 2011), http://www.cio.in/news/rajasthan-village-uses-it-fight-corruption-184592011 (last visited Oct 16, 2011).

includes Mumbai[165], Surat[166], Junagadh[167], Jaipur[168], Ludhiana[169], Hyderabad[170], Bangalore[171], New Delhi[172], Chandigarh[173], Gurgaon[174], Mohali[175], Mysore[176], Vadodara[177], Kolkata[178], Patna[179] etc. The Pune Municipal Corporation even decided to amend its building development laws to require "shopping malls, markets, religious structures, hotels, important tourist attractions, exclusive business buildings, historical buildings and the offices of government and semi-government organisations to install

[165] Bhupen Patel, *CCTVs must for every cyber cafe*, Mumbai Mirror, August 27, 2008, http://m.mumbaimirror.com/index.aspx?Page=article&sectname=News%20-%20Cover%20Story&sectid=15&contentid=20080827200808270239559 49f41f1f9d (last visited Oct 16, 2011).

[166] *Surat police directs public places in Surat to install CCTV*, DNA India, October 11, 2011, http://www.dnaindia.com/india/report_surat-police-directs-public-places-in-surat-to-install-cctv_1597533 (last visited Oct 16, 2011).

[167] *Now, hotels in Junagadh to install CCTVs compulsorily*, Times Of India, July 22, 2011, http://articles.timesofindia.indiatimes.com/2011-07-22/rajkot/29804210_1_guest-houses-cctv-cameras-hotels (last visited Jul 26, 2011).

[168] *Police want CCTVs in city hotels*, Times Of India, July 22, 2011, http://articles.timesofindia.indiatimes.com/2011-07-22/jaipur/29802918_1_hotels-cctvs-reception-and-lobby (last visited Jul 26, 2011).

[169] Sharat Verma, *To keep a close watch, cops urge institutions to install CCTV cameras*, Indian Express, January 7, 2009, http://www.expressindia.com/latest-news/to-keep-a-close-watch-cops-urge-institutions-to-install-cctv-cameras/407461/ (last visited Oct 16, 2011).

[170] Monika Tripathy, *City pubs to keep guests under CCTV surveillance*, THE TIMES OF INDIA, August 31, 2011, http://timesofindia.indiatimes.com/city/hyderabad/City-pubs-to-keep-guests-under-CCTV-surveillance/articleshow/9802801.cms (last visited Oct 17, 2011).

[171] *A drive to ensure CCTV cameras in Bangalore buildings*, DNA India, March 17, 2011, http://www.dnaindia.com/bangalore/report_a-drive-to-ensure-cctv-cameras-in-bangalore-buildings_1520912 (last visited Oct 16, 2011).

[172] *Police ask PCOs, guesthouses to eavesdrop ahead of I-Day*, News24online (2008), http://www.news24online.com/ViewDetails.aspx?NewsId=7095 (last visited Oct 16, 2011).

[173] *Chandigarh banks asked to install police alarms*, Dainik Bhaskar, January 15, 2011, http://daily.bhaskar.com/article/CHD-chandigarh-banks-asked-to-install-police-alarms-1752228.html (last visited Oct 16, 2011).

[174] *Police asks Gurgaon bankers to install CCTV within 3 days*, OneIndia (2008), http://news.oneindia.in/2008/11/20/police-asks-gurgaon-bankers-to-install-cctv-within-3-days-1227193601.html (last visited Oct 16, 2011).

[175] *Banks, showrooms asked to install CCTV cameras*, THE HINDU:, May 19, 2009, http://www.hindu.com/2009/05/19/stories/2009051952840300.htm (last visited Oct 16, 2011).

[176] *Hotel Owners Told to Install Closed Circuit Cameras*, THE HINDU, September 2, 2007, at 03, http://www.hindu.com/2007/09/02/stories/2007090252110300.htm (last visited Oct 16, 2011).

[177] *Notice to malls, multiplexes for not installing CCTVs*, TIMES OF INDIA, October 13, 2011, http://articles.timesofindia.indiatimes.com/2011-10-13/vadodara/30275056_1_cctvs-notices-malls (last visited Oct 16, 2011).

[178] *It's official: colleges on camera -Circular asks principals to install CCTVs to check unrest & illicit activity*, The Telegraph, September 21, 2011, http://www.telegraphindia.com/1110921/jsp/calcutta/story_14532267.jsp (last visited Oct 3, 2011).

[179] Smita Kumar, *Schools cold to lens plan*, THE TELEGRAPH, August 22, 2011, http://www.telegraphindia.com/1110822/jsp/bihar/story_14407130.jsp (last visited Oct 16, 2011).

CCTV cameras"[180]

So a vast apparatus of private surveillance already exists in readiness for the police and other investigative apparatus to tap into. The city of Chennai for instance, reportedly has about 8000 CCTV cameras installed by shops, malls, hospitals and other commercial establishments.[181] Likewise, the Haryana Government is reportedly planning to interlink some 1000 of its own cameras with nearly "20,000 cameras already installed at malls, BPOs, headquarters of multinational companies and markets."[182]

3. Private institutions and associations have, even absent any pressure from police departments, begun installing CCTV surveillance networks of their own. In January 2011, residents of a colony in Gurgaon resolved to install "300 hi-tech CCTV cameras in the colony" According to the scheme, the footage "would be stored in hi-tech gadgets for ten days and would be accessible through the Internet."[183] Diamond Merchants in Surat announced that they would set up a network of 5000 surveillance cameras 'linked to the internet' in three prominent market areas.[184] The Bangalore Jewellers Association decided to impose a fine on all its members who did not have CCTV cameras on their premises.[185] In response to a survey, women commuters on Mumbai's suburban railway network requested the installation of CCTV cameras inside railway coaches.[186] A number of schools and colleges[187] across the country have installed surveillance camera systems

[180] Radheshyam Jadhav, *CCTV cameras in public places will need govt's go-ahead*, TIMES OF INDIA, February 11, 2011, http://articles.timesofindia.indiatimes.com/2011-02-11/pune/28542753_1_cctv-cameras-fire-stations-draft-budget (last visited Oct 16, 2011).

[181] A Selvaraj, *5,000 more CCTV cameras in city - Times Of India*, TIMES OF INDIA, July 15, 2011, http://articles.timesofindia.indiatimes.com/2011-07-15/chennai/29777281_1_cctv-cameras-gold-chain-minor-girls (last visited Oct 16, 2011).

[182] *New security system for Gurgaon, Faridabad*, THE HINDU, November 1, 2011, http://www.thehindu.com/todays-paper/tp-national/tp-newdelhi/article2587270.ece (last visited Nov 1, 2011).

[183] Yogesh Kumar, *300 CCTVs to keep eye on this colony*, TIMES OF INDIA, June 4, 2011, http://articles.timesofindia.indiatimes.com/2011-06-04/gurgaon/29620624_1_cctv-cameras-cctv-installation-colony (last visited Oct 17, 2011).

[184] D.P. Bhattacharya, *Gujarat: 5,000 CCTV cameras for Surat diamond markets*, INDIA TODAY, 2011, http://indiatoday.intoday.in/story/gujarat-5000-cctv-cameras-for-surat-diamond-markets/1/146317.html (last visited Oct 16, 2011).

[185] *Install CCTV, else pay fine*, TIMES OF INDIA, September 26, 2011, http://articles.timesofindia.indiatimes.com/2011-09-26/bangalore/30203663_1_cctv-cameras-theft-cases-jewellery-store (last visited Oct 17, 2011).

[186] Nitasha Natu, *Women on WR want CCTV cams in trains*, TIMES OF INDIA, October 12, 2011, http://articles.timesofindia.indiatimes.com/2011-10-12/mumbai/30270213_1_ladies-compartments-women-commuters-nerul (last visited Oct 17, 2011).

[187] Nimisha Srivastava, CCTV'S IN MUMBAI'S COLLEGE CAMPUSES IBNLIVE (2008), http://ibnlive.in.com/news/cameras-in-colleges-you-cant-bunk-classes/59488-3.html (last visited Oct 16, 2011);

of their own volition for a variety of disciplinary and security reasons. In a tragic incident, a girl committed suicide after she was reprimanded by her college chairman who caught her on CCTV "sitting beside a boy and chatting with him".[188] This move towards surveillance of academic spaces has not been without demur. In May 2010, association of teachers at the Aligarh Muslim University demanded removal of the 70-odd CCTV cameras installed at the campus, on grounds of "unacceptable encroachment into their privacy.[189] Months later, a student of the institution was suspended for spearheading student protests against the move.[190] In September 2010, students of Jadavpur University in Kolkata resisted a move to install CCTV cameras on the university premises.[191]

4. The police in a number of cities have announced ambitious (and expensive) plans of installing city wide networks of surveillance cameras under their own control:
    - In April 2011, the Delhi Police announced plans of augment its existing CCTV surveillance network by adding a further 1045 cameras to the existing stock of 206 cameras (of which 98 were not functional).[192]
    - In June 2011, the city police of Surat announced the installation of 70 CCTVs to

---

Shastry V. Mallady, *CCTV cameras to be installed at university*, THE HINDU, July 29, 2009, http://www.hindu.com/2009/07/29/stories/2009072950370100.htm (last visited Oct 16, 2011); Maroosha Muzaffar, *CCTV cameras to keep watch on city schools*, INDIAN EXPRESS, July 13, 2010, http://www.expressindia.com/latest-news/cctv-cameras-to-keep-watch-on-city-schools/645583/ (last visited Oct 16, 2011); CCTV surveillance to monitor KV-I students, TIMES OF INDIA, July 16, 2011, http://articles.timesofindia.indiatimes.com/2011-07-16/bhubaneswar/29783986_1_cctv-cameras-school-teachers-kvs (last visited Oct 16, 2011); Kumar, *supra* note 154; Delhi University plans to introduce CCTV surveillance from new academic year, INDIA TODAY, May 31, 2011, http://indiatoday.intoday.in/story/delhi-university-plans-to-introduce-cctv-surveillance/1/139887.html (last visited Oct 16, 2011).

[188] *Rebuked for talking to boy, girl kills self*, TIMES OF INDIA, May 29, 2010, http://articles.timesofindia.indiatimes.com/2010-05-29/chennai/28312970_1_hostel-room-college-chairman-college-property (last visited Oct 16, 2011).

[189] *Aligarh Muslim University teachers demand removal of CCTV cameras*, TIMES OF INDIA, May 7, 2010, http://articles.timesofindia.indiatimes.com/2010-05-07/india/28313768_1_cameras-judicial-enquiry-amuta (last visited Oct 17, 2011).

[190] *Student who opposed CCTV at AMU banned for life*, TIMES OF INDIA, July 20, 2010, http://articles.timesofindia.indiatimes.com/2010-07-20/lucknow/28309277_1_campus-ban-cctvs-amu (last visited Oct 17, 2011).

[191] *In JU, students protest against installation of CCTVs on campus*, INDIAN EXPRESS, September 10, 2010, http://www.indianexpress.com/news/in-ju-students-protest-against-installation/679888/ (last visited Oct 17, 2011).

[192] Vijaita Singh, *City's CCTV cameras on the blink, surveillance hit*, INDIAN EXPRESS, April 11, 2011, http://www.expressindia.com/latest-news/citys-cctv-cameras-on-the-blink-surveillance-hit/774381/ (last visited Oct 16, 2011).

monitor roads.[193]

- In July 2011, in the wake of terrorist attacks in Mumbai, several cities decided to install or upgrade their CCTV surveillance networks. The Maharashtra Government announced that it had plans of installing over 5000 cameras – over the 400 existing ones[194] - across the city of Mumbai to meet its security requirements. This figure is inclusive of private security cameras which the police would have access to.[195] The Chennai police, likewise, announced that they planned to install an additional 5000 CCTV cameras in the city.[196] The same month, the city police of Ahmedabad announced that it was setting up 300 advanced IP surveillance cameras in popular spots across the city[197] and the city of Allahabad announced video surveillance in 49 locations.[198] The city of Hyderabad which already had about 225 cameras installed across the city, made a requisition for an additional 600 cameras in the wake of the blasts.[199]

5. Many popular tourist spots in the country are covered by extensive CCTV surveillance, for instance, the Taj Mahal[200], Mecca Masjid at Hyderabad[201], Eliots' Beach in Chennai[202] Nellaiyappar-Gandhimathi Ambal Temple in Tirunelveli[203] Rameswaram

---

[193] *70 CCTV cameras to monitor Surat roads*, DNA INDIA, June 15, 2011, http://www.dnaindia.com/india/report_70-cctv-cameras-to-monitor-surat-roads_1555318 (last visited Oct 16, 2011).

[194] *2000 CCTV cameras in city by year-end*, Indian Express, August 14, 2011, http://www.indianexpress.com/news/2000-cctv-cameras-in-city-by-yearend/831684/ (last visited Oct 16, 2011).

[195] Surendra Gangan, *Maharashtra mulls over London CCTV model for security upgrade*, DNA INDIA, July 19, 2011, http://www.dnaindia.com/mumbai/report_maharashtra-mulls-over-london-cctv-model-for-security-upgrade_1567458 (last visited Jul 26, 2011).

[196] Selvaraj, *supra* note___.

[197] *Now, you will be watched 24X7!*, Times Of India, July 21, 2011, http://articles.timesofindia.indiatimes.com/2011-07-21/ahmedabad/29799245_1_cctv-cameras-electronic-surveillance-city-police (last visited Jul 26, 2011).

[198] Kapil Dixit, *City's 49 locations come under police lens*, THE TIMES OF INDIA, July 25, 2011, http://timesofindia.indiatimes.com/articleshow/9362897.cms (last visited Jul 26, 2011).

[199] *City police seek 600 more CCTV cameras*, Times Of India, July 19, 2011, http://articles.timesofindia.indiatimes.com/2011-07-19/hyderabad/29790471_1_cctv-cameras-cyberabad-police-mumbai-blasts (last visited Oct 16, 2011).

[200] *Watchtowers, CCTV to keep an eye on the Taj Mahal*, MONEYCONTROL.COM (2009), http://www.moneycontrol.com/news/economy/watchtowerscctv-to-keep-eye-taj-mahal_425015.html (last visited Oct 16, 2011).

[201] *New CCTV cameras to keep an eye on Mecca Masjid*, TIMES OF INDIA, July 21, 2011, http://articles.timesofindia.indiatimes.com/2011-07-21/hyderabad/29798975_1_cctv-cameras-mecca-masjid-new-cctv (last visited Oct 17, 2011).

[202] *Elliots Beach comes under electronic eye*, The Hindu, July 3, 2010, http://thehindu.com/news/cities/Chennai/article497133.ece (last visited Nov 30, 2010).

[203] *Surveillance Cameras Installed*, The Hindu, May 20, 2008, at 03, http://www.hindu.com/2008/05/20/stories/2008052055860300.htm (last visited Nov 30, 2010).

Temple[204], etc

6. Apart from providing security against terrorists, CCTVs have been deployed for some years in various cities by traffic police as a routine aid to identifying and apprehending those who violate traffic rules.[205] In many of these cases, the technology includes or is proposed to include automatic recognition of number plates.[206]

From the foregoing account it is clear that video surveillance has become a routine urban phenomena. But what has the impact of CCTVs been in India?

**CCTV Being Watched (SARAI Information Society Project)[207]**

As we sat, sipping cold tea from plastic cups, reminiscing about Ramlal, Gaurav saw a man in khaki filming us with what looked like semi-professional camera. We stopped talking. There we were – three very average specimens of the human race with no glorious/ignominious past nor any such hopes or plans for the future, and this man, this

[204] *Modern CC cameras installed in Rameswaram Temple*, IBN LIVE (2011), http://ibnlive.in.com/news/modern-cc-cameras-installed-in-rameswaram-temple/177869-60-115.html (last visited Oct 16, 2011).

[205] *125 CCTV cams to be installed at traffic junctions in October*, TIMES OF INDIA, September 18, 2011, http://articles.timesofindia.indiatimes.com/2011-09-18/mumbai/30171811_1_junctions-cctv-cams-cameras (last visited Oct 17, 2011); *Traffic police to install CCTV cameras*, TIMES OF INDIA, August 7, 2009, http://articles.timesofindia.indiatimes.com/2009-08-07/chandigarh/28180695_1_cctv-cameras-traffic-police-traffic-congestion (last visited Oct 16, 2011); SUBHASHISH MOHANTY, *CCTV to check capital crime*, THE TELEGRAPH, August 23, 2011, http://www.telegraphindia.com/1110823/jsp/orissa/story_14410685.jsp (last visited Oct 17, 2011); *70 CCTV cameras to monitor Surat roads*, *supra* note___; *12 traffic junctions to have localised CCTV network*, TIMES OF INDIA, August 28, 2010, http://articles.timesofindia.indiatimes.com/2010-08-28/chennai/28298476_1_cctv-cameras-anna-statue-traffic-violations (last visited Oct 16, 2011); Ritesh Shah & Roxy Gagdekar, *Crossed red light? Traffic "eye" to make you pay fine in Ahmedabad*, DNA INDIA, July 23, 2011, http://www.dnaindia.com/india/report_crossed-red-light-traffic-eye-to-make-you-pay-fine-in-ahmedabad_1568582 (last visited Oct 16, 2011); R Rajaram, *Details of over one crore vehicles in VTS database*, THE HINDU, May 3, 2010, http://www.thehindu.com/news/cities/Tiruchirapalli/article420021.ece (last visited Nov 30, 2010); K Ramanujam, *More CCTV cameras to curb road accidents*, DNA INDIA, December 26, 2009, http://www.dnaindia.com/bangalore/report_more-cctv-cameras-to-curb-road-accidents_1327643 (last visited Oct 16, 2011); New system to manage traffic flow in city, TIMES OF INDIA, June 7, 2011, http://articles.timesofindia.indiatimes.com/2011-06-07/chennai/29628703_1_traffic-flow-traffic-police-traffic-violators (last visited Oct 16, 2011).

[206] Ajai Sreevatsan, *Chennai : New system to check violations*, THE HINDU, July 7, 2011, http://www.thehindu.com/news/cities/Chennai/article2203258.ece (last visited Jul 8, 2011); *Elliots Beach comes under electronic eye*, *supra* note___; Raju Parulekar, *In a city of millions, CCTV has no road offences to show*, DNA INDIA, January 23, 2007, http://www.dnaindia.com/mumbai/report_in-a-city-of-millions-cctv-has-no-road-offences-to-show_1076045 (last visited Oct 16, 2011); *Panchkula to install 90 CCTVs*, INDIAN EXPRESS, October 4, 2011, http://www.indianexpress.com/news/panchkula-to-install-90-cctvs/855372/ (last visited Oct 17, 2011); *Third eye to help policemen* , DNA INDIA, August 17, 2007, http://www.dnaindia.com/mumbai/report_third-eye-to-help-policemen_1116009 (last visited Oct 17, 2011).

[207] *CCTV Being Watched*, SARAI, http://www.sarai.net/research/information-society/logs/cctv-being-watched (last visited Nov 1, 2011).

police constable filming us.

What had we done?

This was the first thought that sprung to my mind. We had been learning about cameras, filming perspectives and points-of-view as part of our college curriculum, but here was a man of law, with a revolver hanging down the holster and a camera in his hand, face partially hidden, shooting us!

Enquiries were made and questions about our identity answered. After we confirmed that it was not specially us that he was shooting and that it was routine, we proceeded to ask a few questions – albeit tentatively at first. As law-abiding students of Jamia Millia Islamia University, we thought it wiser not to aggravate the Delhi Police (DP).

Pandu proudly told us that the Delhi Police had initiated this unique programme for citizens' safety and national security. The programme entailed shooting video of 'suspicious characters' (like us!) thronging the New Friends Colony Community Centre market and generating profiles out of the material.

A few days ago, DP had caught an alleged terrorist and he had apparently had dinner here prior to his arrest. Since prevention is better than cure, therefore the drive by the DP to film 'suspicious' looking people, and keep a tab on them. Who knows what they might do when? We saw the footage, appreciated the reality TV-like material and went our way.

I don't know how far this exercise would go in curbing crime, but I, a regular visitor to the Community Centre, avoided the place for a long time.

As an aid to police investigation and to curb traffic violations, CCTV technology has proven invaluable in hundreds of cases across the country. Vindicatory accounts of the use of CCTV technology to apprehend criminals are reported enthusiastically by newspapers and news channels almost on a daily basis. From solving heinous crimes like rape[208] and murder[209], to

[208] *BPO executive held for raping woman in car*, HINDUSTAN TIMES, December 31, 2009, http://www.hindustantimes.com/BPO-executive-held-for-raping-woman-in-car/Article1-492575.aspx (last visited

relatively less serious crimes such as thefts (by far the most numerous of these accounts)[210], traffic rule violations[211] and instances of everyday shoplifting[212], CCTV footage have become a vital input into the forensic apparatus of law enforcement authorities in India. Even where CCTV footage is unavailable at the actual scene of the crime, the police have sought and analysed CCTV footage from the vicinity in a bid to piece together clues.

---

Oct 17, 2011); Divyesh Singh, *CCTVs reduce crime in locality infamous for rapes*, DAINIK BHASKAR, December 14, 2010, http://daily.bhaskar.com/article/cctvs-reduce-crime-in-locality-infamous-for-rapes-1650493.html (last visited Oct 17, 2011).

[209] *Pune police have CCTV footage of murder case suspect*, DNA INDIA, October 16, 2011, http://www.dnaindia.com/mumbai/report_pune-police-have-cctv-footage-of-murder-case-suspect_1599519 (last visited Oct 17, 2011); *Khushi kidnap, murder accused caught on CCTV*, DAINIK BHASKAR, December 1, 2011, http://daily.bhaskar.com/article/CHD-khushi-kidnap-murder-case-murdered-caught-on-cctv-1748337.html (last visited Oct 17, 2011); Sunil Thaplial, *Suspect in toll plaza murder caught on CCTV*, HINDUSTAN TIMES, September 26, 2011, http://www.hindustantimes.com/Suspect-in-toll-plaza-murder-caught-on-CCTV/Article1-750199.aspx (last visited Oct 17, 2011); Gopu Mohan, *CCTV shows people watching as youth is beaten to death*, INDIAN EXPRESS, July 14, 2011, http://www.indianexpress.com/news/cctv-shows-people-watching-as-youth-is-beate/817239/ (last visited Oct 17, 2011); Mihir Tanksale, *Mall CCTV helps cops nab three for techie's murder*, TIMES OF INDIA, February 8, 2010, http://articles.timesofindia.indiatimes.com/2010-02-08/pune/28142652_1_debit-card-katraj-ghat-body (last visited Oct 17, 2011); Nitasha Natu, *Train killer's images caught on CCTV cameras*, TIMES OF INDIA, May 3, 2011, http://articles.timesofindia.indiatimes.com/2011-05-03/mumbai/29498809_1_cctv-cameras-compartment-footage (last visited Oct 17, 2011).

[210] *Caught on CCTV! Foolish security guard stealing from Navi Mumbai flat*, DNA INDIA, October 4, 2011, http://www.dnaindia.com/mumbai/slideshow_caught-on-cctv-foolish-security-guard-stealing-from-navi-mumbai-flat_1594884#top (last visited Oct 17, 2011); *Temple theft: CCTV provides vital clues*, TIMES OF INDIA, January 19, 2010, http://articles.timesofindia.indiatimes.com/2010-01-19/lucknow/28143367_1_vital-clues-forensic-experts-burglary (last visited Oct 17, 2011); Parth Shastri, *CCTV cameras help crack jewellery theft cases*, TIMES OF INDIA, February 16, 2011, http://articles.timesofindia.indiatimes.com/2011-02-16/ahmedabad/28551075_1_cctv-cameras-images-cases (last visited Oct 17, 2011); *Hawk-eyed view: CCTVs IGI help solve thefts*, TIMES OF INDIA, July 5, 2011, http://articles.timesofindia.indiatimes.com/2011-07-05/delhi/29738669_1_cctv-footage-cisf-personnel-airport-management (last visited Jul 8, 2011); *Man installs CCTV, catches thief*, TIMES OF INDIA, April 5, 2010, http://articles.timesofindia.indiatimes.com/2010-04-05/delhi/28119939_1_cctv-footage-theft-accent-car (last visited Oct 17, 2011); *MNC employee, wife held for jewellery theft*, INDIAN EXPRESS, August 1, 2011, http://www.indianexpress.com/news/mnc-employee-wife-held-for-jewellery-theft/825290/ (last visited Oct 17, 2011).

[211] *CCTV effect: 578 cases booked in 10 days*, TIMES OF INDIA, May 26, 2011, http://articles.timesofindia.indiatimes.com/2011-05-26/mysore/29585357_1_traffic-violations-cctvs-notices (last visited Oct 17, 2011); *3rdEye nabs 1,000 traffic violators*, HINDUSTAN TIMES, September 14, 2011, http://www.hindustantimes.com/3rdEye-nabs-1-000-traffic-violators/Article1-745407.aspx (last visited Oct 17, 2011); *UT lists 93 zebra crossing violators*, INDIAN EXPRESS, May 6, 2011, http://www.indianexpress.com/news/ut-lists-93-zebra-crossing-violators/786568/ (last visited Oct 17, 2011); Johnlee Abraham, *Traffic cops fine more with CCTVs in place*, INDIAN EXPRESS, October 21, 2010, http://expressbuzz.com/cities/bangalore/traffic-cops-fine-more-with-cctv-cameras-in-plac/216835.html (last visited Jan 23, 2011).

[212] *18-year-old girl, aunt held in Bandra for shoplifting*, TIMES OF INDIA, October 12, 2010, http://articles.timesofindia.indiatimes.com/2010-10-12/mumbai/28215540_1_shoplifting-cctv-footage-bandra (last visited Oct 17, 2011); *Doctor arrested at airport for shoplifting*, TIMES OF INDIA, August 5, 2011, http://articles.timesofindia.indiatimes.com/2011-08-05/kolkata/29854434_1_cisf-jawan-kolkata-airport-domestic-terminal (last visited Oct 17, 2011); *Shop-lifter caught red-handed on CCTV* , TIMES OF INDIA, January 20, 2011, http://articles.timesofindia.indiatimes.com/2011-01-20/delhi/28354078_1_police-stations-dvd-player-cctv-footage (last visited Oct 17, 2011); Soumittra Bose, *Gang of housewives held for shoplifting*, TIMES OF INDIA, April 6, 2009, http://articles.timesofindia.indiatimes.com/2009-04-06/nagpur/28056184_1_shop-owners-jewellery-shops-shoplifting (last visited Oct 17, 2011).

However, equally numerous accounts appear frequently in the press about the *impotence* of video surveillance. In a revealing disclosure, the Delhi Police in October 2010 revealed that they had solved only one case in the previous three years by using CCTV footage.[213]

Frequently, cameras are found to be dysfunctional or missing within a short period of their installation. Examples of this abound.[214] Thus, for instance,

1. Barely months after they were installed with much fanfare, 13 of the 23 surveillance cameras installed at the Mecca Masjid in Hyderabad were reported not to be functional.[215]
2. In 2008, in an embarrassing incident, 16 surveillance cameras were stolen from the Taj Mahal.[216] After they had been replaced, in December 2010, it was reported that all of the CCTVs in the Taj Mahal had stopped working due to a "virus attack" on their computer systems. The district administration and the police department were apparently in disagreement as to who bore the burden of their maintenance.
3. In March 2011, it was reported that out of the 70-odd CCTV cameras installed in the city of Pune under its Rs. 17 crore "intelligent traffic system" launched the previous year for effective traffic management, only half were still functional. The remaining were being used, not for traffic management, but "primarily for monitoring garbage vehicles, garbage depot, octroi posts and water works".[217]

---

[213] Devesh Pandey, *CCTV cameras not serving much purpose for Delhi Police*, THE HINDU, October 18, 2010, http://www.hindu.com/2010/10/18/stories/2010101860850300.htm (last visited Oct 17, 2011).

[214] Dud cameras in security sieve - Museum employees grilled, no headway in Buddha head theft case, THE TELEGRAPH, December 31, 2004, http://www.telegraphindia.com/1041231/asp/calcutta/story_4193806.asp (last visited Oct 17, 2011); Rajinder Nagarkoti, *Tricity CCTV projects in limbo*, TIMES OF INDIA, April 26, 2011, http://articles.timesofindia.indiatimes.com/2011-04-26/chandigarh/29474230_1_cctv-cameras-cctv-footage-zirakpur-barrier (last visited Oct 17, 2011).("Around 180 CCTV cameras worth more than Rs 35 lakh have been installed across the city but most of those are still not functioning"

[215] *13 CCTVs in Mecca Masjid do not work*, TIMES OF INDIA, August 8, 2011, http://articles.timesofindia.indiatimes.com/2011-08-08/hyderabad/29863808_1_cctv-cameras-mecca-masjid-royal-mosque (last visited Oct 17, 2011).

[216] *Theft at Taj Mahal, close circuit TV cameras go missing*, ONEINDIA (2008), http://news.oneindia.in/2008/05/16/theft-taj-mahal-close-circuit-tv-cameras-missing-1210943160.html (last visited Oct 17, 2011).

[217] Arun Jayan, *"Intelligent" traffic system monitors garbage trucks in Pune*, DNA INDIA, March 23, 2011, http://www.dnaindia.com/mumbai/report_intelligent-traffic-system-monitors-garbage-trucks-in-pune_1523335 (last visited Oct 16, 2011).

4. In April 2011, the Minister for Home Affairs admitted in Parliament that of the 206 CCTV cameras installed at a cost of Rs 75 crore in New Delhi, "98 were not were in a working state".[218]

Even where the cameras are functional, in several cases, the video quality is too poor or indistinct to be of any assistance to law enforcement authorities.[219] In September 2009, ahead of the Commonwealth Games, the Delhi Police complained that "a majority of the 3,000 plus cameras installed at various stadia and venues and connected to Delhi Police central command, communication integrated control room .. to keep a hawk-eyed vigil seem to be "out of focus"."[220]

In other cases, those in charge of CCTV cameras have been negligent either by not switching them on[221], or maintaining backups for reasonable periods. In many cases, cameras have been

[218] Singh, *supra* note___.

[219] *No headway in acid attack case*, TIMES OF INDIA, September 3, 2011, http://articles.timesofindia.indiatimes.com/2011-09-03/chandigarh/30109903_1_acid-attack-cctv-footage-petrol (last visited Oct 17, 2011) ("According to the police, CCTV footage from the petrol pump where the incident took place has been proved inconclusive as the footage was of poor quality."; Shankar Abidi, *J Dey murder: CCTV footage takes police nowhere*, DNA INDIA, June 15, 2011, http://www.dnaindia.com/mumbai/report_j-dey-murder-cctv-footage-takes-police-nowhere_1555108 (last visited Oct 17, 2011) ("The failure of CCTV cameras to give clear images of the killing of investigative journalist J Dey has once again raised concerns about the poor quality of 'hawk eyes' installed in the city."); Joel Joseph, *Poor quality of CCTV led to suspects escaping*, TIMES OF INDIA, September 25, 2011, http://articles.timesofindia.indiatimes.com/2011-09-25/delhi/30200543_1_cameras-toll-plaza-number-plate (last visited Oct 17, 2011) ("We are examining the pictures from the cameras, but the quality of the images is poor because of the bad quality of cameras installed. Ideally the cameras should be able to capture the front and rear images of the vehicle along with the driver's face,"); Dayanand Kamath, *Parel wine shop CCTV record blurred, say police*, DNA INDIA, July 15, 2010, http://www.dnaindia.com/mumbai/report_parel-wine-shop-cctv-record-blurred-say-police_1409909 (last visited Oct 17, 2011).

[220] Rahul Tripathi, *CCTV cameras at venues out of focus*, TIMES OF INDIA, September 29, 2010, http://articles.timesofindia.indiatimes.com/2010-09-29/delhi/28242854_1_cctv-cameras-ecil-venues (last visited Oct 17, 2011).

[221] *Burglary in jewellery shop, Rs 21L worth property stolen*, TIMES OF INDIA, October 19, 2010, http://articles.timesofindia.indiatimes.com/2010-10-19/hyderabad/28265156_1_cctv-cameras-jewellery-shop-jewellery-store (last visited Oct 17, 2011); Arun Dev, *All that glitters is low security*, TIMES OF INDIA, July 9, 2011, http://articles.timesofindia.indiatimes.com/2011-07-09/bangalore/29755105_1_cctv-cameras-security-systems-jewellery-shop-owners (last visited Jul 12, 2011). (During a robbery in Bangalore in June 2011, "two assailants came to a jewellery store and attacked its owner Prakash Chaudhary and his assistant Surendhar, and fled with Rs 10 lakh worth of gold. On that Monday, Prakash had forgotten to switch on the CCTV camera.")

installed by the police "without recording facility"[222] or without networking them to a central office.[223]

Despite the proliferation of CCTVs, as evident from the foregoing account, there are no laws that govern their deployment or use in India – either by the government or in the private sector. The closest applicable law concerns electronic voyeurism and is contained in Section 66E of the IT Act which penalizes the "capturing, publishing and transmission" of images of the "private area"[224] of any person without their consent, "under circumstances violating the privacy" of that person. This last phrase has been explained as meaning "circumstances in which a person can have a reasonable expectation that (i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured or (ii) any part of his or her private area would not be visible to the public regardless of whether that person is in a public or private place". [225] This offence is punishable with imprisonment of up to three years or with a fine of up to Rs. Two lakh rupees or both.

Although India currently does not have the roughly 1.85 million CCTVs that Britain reportedly has[226], we are making rapid, and unthinking strides to make up the shortfall. Certainly the CCTV industry is gearing up to provision the government, should it choose to embark on this course, for a program of total surveillance. Nor is there a dearth in demand for this surveillance – as indicated above, there is general consensus among the public of both the desirability and utility of CCTV cameras in preventing crime and particularly in forestalling terrorism. Over the past few years, each successive terrorist attack incident has fuelled a new round of frenzied CCTV purchase by the government under the censorious gaze of the media. In their portrayal of the absence of CCTV cameras as a lack of serious commitment to security, and by providing mesmerising accounts of the state's plans to install hundreds and thousands of such cameras, the

---

[222] Sunchika Pandey, *No recording facility in CCTV, cops tell RTI applicant*, DNA INDIA, Monday, Jan 31, http://www.dnaindia.com/mumbai/report_no-recording-facility-in-cctv-cops-tell-rti-applicant_1501101 (last visited Oct 17, 2011); *Dud cameras in security sieve - Museum employees grilled, no headway in Buddha head theft case*, *supra* note___.

[223] Pandey, *supra* note___.

[224] 'Private area' has been defined in the Explanation to Section 66E as "the naked or undergarment clad genitals, pubic area, buttocks or female breast".

[225] See Explanation to Section 66E IT Act 2000 (2008 Am)

[226] *One CCTV camera for every 32 people in Big Brother Britain*, THE MAIL, March 3, 2011, http://www.dailymail.co.uk/news/article-1362493/One-CCTV-camera-32-people-Big-Brother-Britain.html (last visited Oct 17, 2011).

media have played a catalyst role in this march towards a surveillance-state that India has currently begun.

To be sure, the availability of CCTV footage – instant proof - has been an ally to the otherwise rather slothful police apparatus in India. In a country with a conviction rate hovering around 41% with over 7 million criminal cases pending trial, and with only 1.3 policemen per 1000 civilians[227], the promise of CCTV aided law-enforcement carries a particularly optimistic charge.

As a privacy advocate, concerned by these developments, one can perhaps take solace, however small, in the fact that the totalitarian ambitions of the state do not always come to pass and are routinely thwarted by such allies of privacy as corruption, inefficiency, forgetfulness, neglect and ordinary wear and tear.

## §15 Restrictions on Internet use, cybercafes

According to a report by the Internet & Mobile Association of India titled 'I-Cube 2009-2010: Internet in India', 37% of all internet usage in India occurs through cyber-cafes.[228] Despite the figures in this report, there is a sense that cyber cafes are on the decline in urban areas due to a combination of factors such as the rise of broadband, lowering of prices of PCs and the high costs of real estate.[229]

An additional reason for their decline could also be the onerous restrictions that have been imposed on cyber-cafes in various states - most recently through rules notified under the Information Technology Act in 2011. Cyber cafes are viewed with deep suspicion by the law enfocement apparatus in India, and tend to be seen as sites that promote criminal activity. This has led to the imposition of a range of restrictions on them – from requiring cyber cafes to obtain registration before opening business to requiring them to maintain detailed logs of users, requiring them to use internet filters, restrictions on the geometry of cubicles etc.

---

[227] CRIME IN INDIA - 2009 1,5,164 (2010), http://ncrb.nic.in/CII-2009-NEW/Compendium2009.pdf (last visited Oct 3, 2011).

[228] Arun Prabhudesai, 52 MILLION ACTIVE INTERNET USERS IN INDIA – RURAL INDIA OVERTAKES URBANITES TRAK.IN (2010), http://trak.in/tags/business/2010/04/07/internet-usage-india-report-2010/ (last visited Oct 10, 2011).

[229] Nikhil Pahwa, REASONS FOR THE DECLINING GROWTH OF CYBERCAFES IN INDIA MEDIANAMA (2008), http://www.medianama.com/2008/07/223-reasons-for-the-declining-growth-of-cybercafes-in-india/ (last visited Oct 10, 2011).

Simultaneously the government has attempted to curb the freedom of expression online through new regulations which expose 'intermediaries' to liability unless they assist government agencies in tracking down individual users who post a range of officially unwanted content.

In this section we provide an overview of the restrictions placed on internet use and on cyber cafes.

Section 79 of the IT Act grants immunity from liability to 'intermediaries' for third party content made available or hosted by them, provided, inter alia, the intermediary observes 'due diligence' and follows prescribed norms. As noted previously the IT Act contains a very expansive definition of 'intermediaries'. In 2011, the Ministry of Information and Technology issued two sets of rules under this Act – one to govern intermediaries such as ISPs and web-platforms, and another set to govern cyber cafes. These rules severely attenuate both the freedom of expression of citizens and their right to privacy.

## 15.1 Intermediary 'Due Diligence' Rules

As noted above, one of the requirements for immunity from liability is that intermediaries observe 'due diligence'. In April 2011, the Government issued rules defining the 'due diligence' measures intermediaries are required to observe. According to these rules, intermediaries must incorporate into their terms of service, the warning that users are forbidden from publishing the following categories of information:

(a) belongs to another person and to which the user does not have any right to;

(b) is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;

(c) harm minors in any way;

(d) infringes any patent, trademark, copyright or other proprietary rights;

(e) violates any law for the time being in force;

(f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;

(g) impersonate another person;

(h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;

(i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation

Within 36 hours of obtaining knowledge of any such information being transmitted through its networks, an intermediary is required to take steps to 'disable such information'. Further, the intermediary is required to provide assistance to government agencies "purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law".

These rules have been widely condemned as being unlawful since they are both ultra vires Section 79 of the IT Act under which they have been made as well as the Constitution of India which guarantees the freedom of speech and expression.[230]

## 15.2 Cyber Café Rules

Along with the Due Diligence Rules, the Ministry also notified separate rules to be adhered to by Cyber Cafes[231]. Like the word 'intermediary', Cyber-café has a very broad definition under the IT Act and means "any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public".[232] As is evident, this definition includes not just conventional cyber-cafes, but also a host of other venues where internet may be accessed including hotels, airport lounges etc. According to the new rules, cyber cafes are forbidden from allowing any user to use their computer resources "without the identity of the user being established.". A user may establish his identify by producing any of 7 different identity documents including driving license, passport etc. The Cyber Café is required to keep a copy – either scanned or photocopy - of the identity document produced and such copy is to be retained for a period of one year. In addition, the cyber café 'may' photograph a user using a

[230] CIS Para-wise Comments on Intermediary Due Diligence Rules, 2011, Centre for Internet and Society (2011), http://www.cis-india.org/internet-governance/blog/intermediary-due-diligence (last visited Oct 15, 2011).

[231] Information Technology (Guidelines for Cyber Cafe) Rules, 2011, http://www.mit.gov.in/sites/upload_files/dit/files/GSR3_10511%281%29.pdf (last visited Oct 15, 2011).

[232] Section 2(na) of the Information Technology Act, 2000 (as amended in 2008).

'web camera' and such photograph would be included in the log register maintained by the cyber café.

The Cyber Café is required to maintain a detailed log of every user that includes the following information : (ii) Name (iii) Address (iv) Gender (v) Contact Number (vi) Type and detail of identification document (vii) Date (vii) Computer terminal identification (viii) Log in Time (ix) Log out Time. For at least one year, the cyber café must also retain the complete History of websites accessed using computer resources at the cyber café and all logs of proxy server installed at cyber cafe.[Rule 5] The rules require that all computers "may" be equipped "with commercially available safety or filtering software"

Not content with mere electronic surveillance, the rules also stipulate the size of cubicles and their orientation.

Any officer authorized by the government has powers to check and inspect cyber cafes and the log registers maintained at any time.

As with the Due Diligence rules, these rules have come under heavy fire for their draconian content from civil society commentators and bloggers.[233]In its reply to the draft version of these rules, PrivacyIndia/Center for Internet and Society had pointed out that the rules gravely imperil privacy by requiring extensive logs to be maintained of every user.[234] Previous state-level regulations of this kind have exposed cyber-café owners to undue hardships and harassment at the hands of local police while not leading to a corresponding increase in security.[235] In other cases, in the absence of a monitoring mechanism, the cyber cafes have, under government regulation, accumulated vast logs without any actual oversight ever occurring.[236] In both cases, unfortunately, it is privacy of the individual that has ultimately suffered as copies of increasing numbers of ID documents accumulate in the hands of cyber café owners, mobile phone agents etc. Already a cottage industry of fake identity documents has mushroomed due to this

[233] *See* Nikhil Pahwa, INDIA'S CYBERCAFE RULES FINALIZED; FOUNDATION FOR HARASSMENT MEDIANAMA (2011), http://www.medianama.com/2011/05/223-india-cyber-cafe-law/ (last visited Oct 15, 2011).
[234] CIS Para-wise Comments on Cyber Café Rules, 2011, CENTRE FOR INTERNET AND SOCIETY (2011), http://www.cis-india.org/internet-governance/blog/cyber-cafe-rules (last visited Oct 15, 2011).
[235] *1,200 cyber cafes, one valid licence*, INDIAN EXPRESS, August 5, 2008, http://www.expressindia.com/latest-news/1-200-cyber-cafes-one-valid-licence/344737/ (last visited Oct 15, 2011).
[236] Shalabh Manocha, *Cops no more interested in checking cyber cafes*, TIMES OF INDIA, August 3, 2009, http://articles.timesofindia.indiatimes.com/2009-08-03/lucknow/28172232_1_cyber-cafe-proper-records-ip-address (last visited Jun 28, 2011).

promiscuous availability of ID documents. In August 2011, the Economic Times reported on the existence of a "Fake ID market" in Mumbai where the going rate for an ID proof was as low as "Rs 5 for an ID proof with an original photograph, and Rs 50 for an ID with an original photograph and two supporting documents " The article goes on to report that "In just the past six months, 54 FIRs have been registered against several retailers, cutting across a spectrum of service providers, for stealing a customer's identity and then using it to issue multiple SIM cards to multiple customers."[237] Far from this being a solitary occurrence, this seems to have become a widespread phenomenon across the country with similar incidents having been reported in West Bengal[238], Hyderabad[239], Patiala[240], Lucknow[241] and New Delhi[242] among other places. Most often when these scams are 'unearthed' the harms to privacy of citizens are dulled by an overriding discourse of national security which presents these incidents primarily as aids to terrorism. It is here that perhaps a critique based on the citizen's privacy could prove most beneficial since it would, perhaps more than one founded on national security, reveal the complicity of the state in begetting this fake identity market. By forcing people to deal promiscuously with their identity documents in order to secure basic telephony and internet services, the state has unwittingly created the conditions for the flourishing market of fake documents we witness today. In its pursuit of the white whale of 'national security' – supposedly secured through scrupulous verification of identity documents – the state has created the conditions for a situation where practically *nobody's* identity document is credible anymore since

[237] Yogesh Sadhwani, *Mobile companies misuse your personal documents*, ECONOMIC TIMES/MUMBAI MIRROR, August 11, 2011, http://articles.economictimes.indiatimes.com/2011-08-11/news/29876366_1_sim-cards-id-proof-vodafone-application (last visited Oct 23, 2011).

[238] *Both SIM & proof for a "little" extra*, THE TELEGRAPH, November 27, 2010, http://www.telegraphindia.com/1101127/jsp/siliguri/story_13227939.jsp (last visited Oct 23, 2011). Reporting that "During simultaneous searches ..police seized ..blank Customer Application Forms (CAFs) affixed with photographs of unknown persons, 473 passport size photographs, photocopies of ID and residence proofs like ration cards and driving licences."

[239] *Illegal SIM card racket busted*, TIMES OF INDIA, August 13, 2010, http://articles.timesofindia.indiatimes.com/2010-08-13/hyderabad/28313020_1_sim-cards-customer-application-forms-proofs (last visited Oct 23, 2011).

[240] *Three held for giving fake cell connection*, TIMES OF INDIA, October 28, 2008, http://articles.timesofindia.indiatimes.com/2008-10-28/delhi/27917475_1_sim-cards-cyber-cafe-identity-cards (last visited Oct 23, 2011).

[241] *Over 1,600 activated SIMs seized, two held*, TIMES OF INDIA, September 5, 2010, http://articles.timesofindia.indiatimes.com/2010-09-05/lucknow/28231237_1_sims-mobile-shop-fake-identity-proofs (last visited Oct 23, 2011).

[242] *Three held for giving fake cell connection*, TIMES OF INDIA, October 28, 2008, http://articles.timesofindia.indiatimes.com/2008-10-28/delhi/27917475_1_sim-cards-cyber-cafe-identity-cards (last visited Oct 23, 2011).

there are too many fakes floating around. Perhaps nothing more serves to illustrate the urgent need in India to build privacy concerns into state policy at the planning stage itself.

## §16 Cyber security

In April 2011, the Ministry of Information Technology released a draft Cyber Security Policy which talks in general terms about "deployment of technologies and capabilities for real-time protection and incident response", the need for "cyber intelligence and cyber intelligence" and the need for preparedness at all levels. The policy has still not been finalized and contains no discernible privacy implications. [243]

The IT Act confers vast powers of interception and monitoring under Sections 66-69 of that Act. These powers extend to issuing directions requiring any person in charge of a computer to extend all facilities to decrypt information. In other words, the government may hack in order to gain access to information which it lawfully requires.

Section 66 of the IT Act creates a broad offence of "dishonestly or fraudulently" hacking, tampering with source code etc. which even applies to the government. i.e. Even the government can be prosecuted if it hacks a computer system if it can be shown to have acted dishonestly or fraudulently. However, this is subject to Section 84 of the IT Act which immunizes actions by officials undertaken in good faith and in pursuance of the provisions of the Act.

## §17 Administrative Issues

India does not yet have a mandatory ID Card – in the sense of a document that must, by law be produced to authorities on demand, failing which a person may be detained. I.e. failure to produce an identifying document is itself not an offence. However this statement is qualified by two facts: Firstly, the government is currently undertaking an exercise under the Citizenship Act to mandatorily register citizens (see National Population Register below) and *secondly*, that in certain conflict-ridden states of India – the entire North East and Jammu and Kashmir, for instance – the army and the police have been given extraordinary powers including arresting without warrant. In these areas failure to carry and produce upon demand valid ID documents

[243] NATIONAL CYBER SECURITY POLICY - DISCUSSION DRAFT (2011), http://www.mit.gov.in/sites/upload_files/dit/files/ncsp_060411.pdf (last visited Oct 17, 2011).

can have serious implications. As one commentator notes in relation to Jammu and Kashmir, "Movements of people on roads and bazar is regulated with frequent demands to show their IDs and frisking and searching of bags. It is a known fact that anyone in area declared "Disturbed" found without a ID can suffer anything from having to bribe his way to freedom to becoming a victim of enforced disappearance."[244]

Given the trajectory of "security measures" in India, it would not be unfair to say that we are one major terrorist attack away from a generalized compulsory identification system.

Even otherwise, the police in India have vast powers of arrest in the case of cognizable offences and may in certain cases provided under Section 151 of the Code of Criminal Procedure (CrPC), arrest without a warrant. Section 42 of the CrPC permits the police to arrest a person "who has committed an offence in the presence of a police officer or has been accused of committing a non-cognizable offence" and refuses, on demand being made by a police officer to give his name and residence or gives false name or residence. Such a person may be arrested only for the limited purpose of ascertaining his name and residence.[245]

As the Law Commission has observed," The vast discretion given by the CrPC to arrest a person.. clothe the police with extraordinary power which can easily be abused.. Neither there is any in-house mechanism in the police department to check such misuse or abuse nor does the complaint of such misuse or abuse to higher police officers bear fruit except in some exceptional cases.

Foreigners registered under the Foreigners Act (see Sec. 9 above) are required upon demand "by any Registration Officer, any magistrate or any police officer not below the rank of a head constable" to produce their certificate of registration and other identity documents.[246]

In 2008, the Ministry of External Affairs began issuing RFID chip enabled 'e-passports' to select officials in the government. Although the plan was to extend this facility to the general population starting in 2009, successive delays in implementation have prevented a full-scale

[244] Gautam Navlakha, *Principled versus Piecemeal Approach: Repeal of AFSPA, Troops Pullout or Ending War against our People*, SANHATI (November 2010), http://sanhati.com/excerpted/2913/ (last visited Oct 18, 2011).
[245] Similar powers or arrest for failure to disclose name and residence are granted in several statutes such as state Forest Laws, Excise laws etc. In each of these cases, the person must be "reasonably suspected" of having committed an offence under the empowering Act.
[246] General Requirements For Registration Of A Foreign National, *supra* note___.

unrolling of this project. There are rumours that the project has stalled due to allegations that Gemalto, the multi-national company selected to supply the chips and software[247] for the e-passports, had links with Pakistan's spy agency – the Inter-Services Intelligence. The project is reportedly awaiting clearance from the home ministry and the ministry of defence. [248]

In the past decade there have been two kinds of attempts at providing identity cards. First, various states have issued ad-hoc identity documents for a variety of purposes including to secure employment and food supplies. Secondly, the Central Government has hatched schemes – not always successfully - to provide Pan-indian Identity documents to all citizens. In the remainder this section we examine, briefly, examples and careers of both kinds of documents.

## 17.1 State-level Identity Cards

> "[A] scam was unearthed in the Public Distribution System in Panchmahals district, where 1.1 lakh bogus [biometric] ration cards were found during a scrutiny recently."
>
> The Indian Express (July 2011)[249]

Due to the federal setup of our constitution, the administration of most welfare schemes – from employment guarantee to disability pension and food rations - tends to be the responsibility of the various state governments. And, obeying the inexorable market logic of India in the 21st century, in the past decade, practically each such welfare scheme in each state has spawned its own identity document. Perhaps the most ubiquitous of these is the ration card which entitles families to specified monthly allocations of food grains and other supplies. These ration cards have traditionally been used in India as Identity documents for a range of corollary transactions such as obtaining a gas, electricity or a telephone connection. In the past few years, most states have either announced or implemented schemes to convert these paper documents into biometric cards with, as the news report above indicates, mixed results.

---

[247] *Government of India selects Gemalto to jump-start electronic passport program*, FINANCIAL EXPRESS, September 17, 2008, http://www.financialexpress.com/news/government-of-india-selects-gemalto-to-jumpstart-electronic-passport-program/362552/0 (last visited Oct 23, 2011).

[248] Sahil Makkar, *E-passport project delayed over allegations against tech provider*, LIVEMINT, March 24, 2011, at 4, http://www.livemint.com/articles/2011/03/23214058/Epassport-project-delayed-ove.html?atype=tp (last visited Oct 23, 2011).

[249] *Post-scam, 2.5 lakh ration cards now under scrutiny*, INDIAN EXPRESS, July 11, 2011, http://www.indianexpress.com/news/postscam-2.5-lakh-ration-cards-now-under-s/815733/ (last visited Oct 23, 2011).

In August 2010, Orissa began collecting biometric data including finger prints and iris scans from citizens.[250] The State of Karnataka has reportedly already issued biometric bar-coded ration cards to "74 lakh households" in the state between 2008-2011. [251]In the past year alone, the states of Goa[252], Tamil Nadu[253], Rajasthan[254], Maharashtra[255] Haryana[256], have all announced plans to distribute biometric ration cards to all residents of those states. In a curious display of pioneerism, each state unfailingly declares itself to be the 'first state in the country' to have introduced this facility.[257]

In addition, the states also issue driving licenses through their respective Transport Departments. Although in the past, inadequate interlinking between state departments prevented driving licenses from becoming a 'national id', recent measures by the central government, including the mandating of smart-card based driving licenses by December 2009[258] and the setting up of a National Registry of Licenses have imbued locally issued licenses with a national character. In addition, there are plans to issue all driving licenses in the Union of India's name.[259] In July 2010, the Union Ministry of Road Transport announced the establishment, within 6 months, of a 'national registry of all driving licenses' which envisaged the interlinking of all state transport departments to prevent duplicate licenses from being issued. The purpose of the National

[250] Debabrata Mohanty, *In India's heart of darkness, biometric ration card is flicker of hope for a million*, INDIAN EXPRESS, August 23, 2010, http://www.indianexpress.com/news/in-indias-heart-of-darkness-biometric-ration-card-is-flicker-of-hope-for-a-million/663778/0 (last visited Oct 23, 2011).
[251] Prabhu, *supra* note___.
[252] *Smart-card project for ration quotas revived*, TIMES OF INDIA, August 4, 2011, http://timesofindia.indiatimes.com/city/goa/smart/card-project-for-ration-quotas-revived/articleshow/9474367.cms (last visited Oct 23, 2011).
[253] *Ration cards to go biometric to weed out fakes*, TIMES OF INDIA, August 20, 2011, http://articles.timesofindia.indiatimes.com/2011-08-20/chennai/29909152_1_ration-cards-biometric-fakes (last visited Oct 23, 2011).
[254] *Biometric ration cards soon: Minister*, TIMES OF INDIA, August 12, 2011, http://articles.timesofindia.indiatimes.com/2011-08-12/jaipur/29879683_1_ration-cards-fair-price-bpl-card-holders (last visited Oct 23, 2011).
[255] Rakshit Sonawane, *Maharashtra plans biometric ration cards*, INDIAN EXPRESS, January 7, 2010, http://www.indianexpress.com/news/maharashtra-plans-biometric-ration-cards/564413/ (last visited Oct 23, 2011).
[256] Deepender Deswal, *Smart cards to replace ration cards in Haryana*, TIMES OF INDIA, May 16, 2011, http://articles.timesofindia.indiatimes.com/2011-05-16/india/29547947_1_smart-cards-ration-cards-village (last visited Oct 23, 2011).
[257] *Id.*
[258] *Dec 31 deadline for smart card-based driving licences*, TIMES OF INDIA, September 25, 2009, http://articles.timesofindia.indiatimes.com/2009-09-25/india/28082944_1_smart-card-based-licences-and-vehicle-registration-uts (last visited Oct 23, 2011).
[259] *Now, driving licences to be issued in Union of India's name*, TIMES OF INDIA, July 21, 2011, http://articles.timesofindia.indiatimes.com/2011-07-21/india/29799212_1_licences-transport-sector-rto (last visited Oct 23, 2011).

Register would "information to the department of road transport and highways, RTOs, inter-state check posts and the police for quick verification of documents and information."[260] The registry 'www.vahan.nic.in' was officially inaugurated a year later in July 2011 and includes details of Details of "about 90 lakh vehicles, including complete information about owners, tax payment and permit, and about 80 lakh driving licences are available." [261]

In May 2011, the state of Gujarat announced plans to launch its own Identity card project to rival the Aadhar project of the Central Government (see below). Accordingly to news reports, the project would "give every individual an UID number and have details such as if the person is below or above the poverty line, whether he/she pays income tax, permanent address, property ownership and if entitled to reservation benefit."[262]

## 17.2 Central Identity Schemes

### 17.2.1 The Permanent Account Number Card

The Permanent Account Number (PAN) is a ten-digit alphanumeric number, issued by the Income Tax Department in India specifically to facilitate the interlinking of all financial transactions related to a specified person. According to a document on the Department's website, "PAN enables the department to link all transactions of the "person" with the department. These transactions include tax payments, TDS/TCS credits, returns of income/wealth/gift/FBT, specified transactions, correspondence, and so on. PAN, thus, acts as an identifier for the "person" with the tax department"[263]

Although introduced in 1995, the PAN was made mandatory in January 2005 and it is compulsory to quote this number in most high value transactions exceeding Rs. 50,000 and

[260] Dipak Kumar Dash, *National registry of licences in 6 months*, TIMES OF INDIA, July 19, 2010, http://articles.timesofindia.indiatimes.com/2010-07-19/india/28319958_1_rtos-licences-registry (last visited Oct 23, 2011).
[261] Anil Kumar Sastry, *Get details of vehicles at the click of a mouse*, THE HINDU, August 14, 2011, http://www.thehindu.com/todays-paper/article2355480.ece (last visited Oct 23, 2011); *National register to help track stolen vehicles from today*, TIMES OF INDIA, July 20, 2011, http://articles.timesofindia.indiatimes.com/2011-07-20/india/29794140_1_rtos-dealers-and-police-department-licences (last visited Oct 23, 2011).
[262] *Gujarat launches its own UID project*, ECONOMIC TIMES, May 11, 2011, http://articles.economictimes.indiatimes.com/2011-05-11/news/29532284_1_uid-project-pilot-project-ration-cards (last visited Oct 23, 2011).
[263] What is PAN, (2010), http://www.incometaxindia.gov.in/archive/About%20PAN_06302010.pdf (last visited Oct 24, 2011).

certain other specified transactions such as applying for a telephone or opening a bank account, payments to hotels exceeding Rs. 25,000.[264]

Section 139A of the Income Tax Act forbids persons from obtaining more than one PAN Number.

Failure to comply with the provisions – failure to obtain a PAN Number and quote it during transactions - could lead to an imposition of a penalty of Rs. 10,000. (Sec 272B). (Failure to quote PAN numbers, although technically illegal, however, appears only to be pursued and penalized by the IT Department in cases where the value exceeds Rs. 25 lakh.[265])

Unlike the Social Security Number in the US, the avowed purpose of the PAN system is to interlink various transactions of a person in order to gather intelligence about their activities. The Central Information Branch, the intelligence wing of the Central Board of Direct taxes , newly revamped in 2010 to "ensure current, constant and consolidated reporting and delivery of information on transactions" [266] has recently put in place "software that already has extensive information on taxpayers mapped to their respective PAN cards"[267]

In 2006, the then Finance Minister Chidambaram, proposed a plan to issue biometric PAN cards which "would have carried the I-T assessees' fingerprints (two from each hand) and the face."

---

[264] For a full list of transactions requiring the quotation of PAN Number, see Rule 114B of the Income Tax Rules. RULE 114B, INCOME TAX RULES, http://law.incometaxindia.gov.in/DIT/HtmlFileProcess.aspx?page=ITRU&schT=rul&csId=21533008-bbb4-4f86-b609-9296e8b5223e&rNo=114B&sch=&title=Taxmann%20-%20Direct%20Tax%20Laws (last visited Oct 24, 2011).

[265] Shruti Srivastava, *Expect summons from I-T dept for non-PAN transactions*, INDIAN EXPRESS, June 6, 2011, http://www.indianexpress.com/news/expect-summons-from-it-dept-for-nonpan-tra/799748/ (last visited Oct 24, 2011). ("The department issued letters to over two lakh such cases where the transaction value exceeded Rs 25 lakh. But in 57,000 cases, letters could not be served due to wrong addresses and "deliberate wrong information".In another one lakh cases, the department did not receive any reply though letters were served.")

[266] *Finmin overhauls I-T intelligence to counter tax evasion*, ECONOMIC TIMES, January 24, 2010, http://articles.economictimes.indiatimes.com/2010-01-24/news/28463188_1_intelligence-wing-tax-evasion-income-tax (last visited Oct 24, 2011). Reporting that "The CIB is the nodal office in the department to gather all documents pertaining to transactions in relation to which Permanent Account Number (PAN) or General Index Register Number are given during sale and purchase of property and monetary deposits. "*The re-structuring of the Central Information Branch will ensure current, constant and consolidated reporting and delivery of information on transactions, including high value financial ones* which are around Rs 10 lakhs or more," sources said.""

[267] Deepshikha Sikarwar, *IBA and CBDT join hands to fight black money*, ECONOMIC TIMES, August 27, 2011, http://articles.economictimes.indiatimes.com/2011-08-27/news/29934851_1_income-tax-bank-accounts-black-money (last visited Oct 24, 2011).

However, with the announcement of the more ambitious UID project (see below) and the transfer of the minister to the Home Ministry, this plan was put on hold.[268]

In May 4, 2011, the Finance Ministry announced measures to streamline the financial information provided by third parties – such as banks and mutual fund companies - to the CBDT to facilitate smoother and faster access to information about persons.[269]

In August 2011, the IBA (the Indian Banks' Association) representing "more than 160 Indian and foreign banks operating in the country" agreed to provide access to banks' data bases with the Central Board of direct taxes – purportedly in order to check the accumulation of black money. This move, it is stated, would give tax authorities "a 360 degree view of the taxpayer." [270]

Despite the aspiration of the system to achieve total financial e-supervision of all persons in India, these totalitarian ambitions have been thwarted by rampant counterfeiting of pan cards.[271] In a revealing report the Comptroller and Auditor General of India (CAG) tabled a report for 2010-11 on Direct Taxes in Parliament revealing that "958 lakh PANs were issued up to March 2010 but IT returns filed in the last fiscal were only 340.9 lakh". The CAG report suggested "issuance of multiple PAN cards" as a possible reason for this large discrepancy.[272]

As noted previously, the linking of PAN cards as a condition to accessing a variety of quotidian services has created the necessary conditions for the wholesale counterfeit market we witness

---

[268] *Biometric PAN cards put on hold*, DECCAN HERALD, April 4, 2010, http://www.deccanherald.com/content/62050/biometric-pan-cards-put-hold.html) (last visited Oct 31, 2011).

[269] "Currently, most high-value transactions are reported to the Income-Tax department through two channels — Annual Information Return (AIR) and Central Information Branch (CIB)..CIB collects information relating to specified transactions for which Permanent Account Number (PAN) is mandatory, such as bank deposits above Rs 50,000, property deals above Rs 5 lakh, sale or purchase of a vehicle, opening a bank account..AIR, on the other hand, is furnished by banks, financial institutions, trustees of mutual funds, companies issuing bonds or debentures, " Vrishti Beniwal, *Black money info sources to be merged*, BUSINESS STANDARD, May 4, 2011, http://www.business-standard.com/india/news/black-money-info-sources-to-be-merged/434400/ (last visited Oct 24, 2011).

[270] Sikarwar, *supra* note___.

[271] *Hi-tech scam busted*, TIMES OF INDIA, April 29, 2008, http://articles.timesofindia.indiatimes.com/2008-04-29/mumbai/27750367_1_credit-cards-pan-cards-software-engineer (last visited Oct 24, 2011); *Two held for making fake identity cards, licenses*, TIMES OF INDIA, June 22, 2008, http://articles.timesofindia.indiatimes.com/2008-06-22/chennai/27748686_1_pan-cards-identity-cards-passports (last visited Oct 24, 2011); Rakesh Sonawane, *Fake document racket busted in Ulhasnagar, 4 held*, HINDUSTAN TIMES, July 21, 2011, http://goo.gl/fxWi5 (last visited Oct 24, 2011); *Forgery racket busted*, 1 arrested, DAINIK BHASKAR, March 4, 2011, http://goo.gl/4vERp (last visited Oct 24, 2011).

[272] *Ensure a tax payer gets only one PAN: CAG to I-T dept*, ECONOMIC TIMES, March 18, 2011, http://articles.economictimes.indiatimes.com/2011-03-18/news/29141734_1_pan-card-tax-payer-permanent-account-number (last visited Oct 24, 2011).

today. With the failure of each successive form of ‘foolproof’ ID, the state rushes blindfolded into the next newest available technology in the hope of finding redemption. Paradoxically, as the webs of generalized surveillance intensify through such measures as the interlinking of databases, international tax information sharing etc, there is no corresponding sense of more and bigger criminals being brought to book. To the contrary, criminality seems to be increasing in an accelerative manner with new forms of illegality spawning out of precisely the same technologies that the state nourishes and depends on. In the era of the biometric card, video surveillance and the smart card, the identity of the individual seems as protean as ever – perhaps more so, since, in the age of mechanical reproduction, one does not ever *truly* know how many fakes of one’s identity document are floating around, how many mobile connections have been issued in one’s name or how many cyber-cafés one’s ID card has visited. With the state requiring identity to be established routinely for accessing most quotidian services, the ID document itself has transformed in the lay, non-elite perception into merely an additional transaction cost that must be borne as a condition for doing business in India.

With each paranoid stumble the state makes towards greater technological protection, one cannot suppress a sense that in the same move, privacy takes a step backwards.

Perhaps one important intervention in favour of privacy could be a statutory *reduction* in the number of transactions that require identity documents for their access. At the very least this would reduce the number of opportunities a 'potential terrorist – the bête noire par excellence of the state, but also its prime citizen since all executive action is conducted in his name and bearing him in mind - would have to obtain false documents. At present this task is his simplest – and a culture – emerging out of conditions set by the state - that condones false documents, even sees them as indispensible to living can only aid him further.

### 17.2.2 The Electoral Voter ID Card

The Election Commission of India (ECI) is a permanent constitutional body responsible for overseeing the conduct elections in India. One of the functions of the ECI is to prepare electoral rolls of registered voters in all assembly constituencies in India and more recently, to issue photo Identity cards (EPIC) to all voters. For this purpose, a registration officer may access and requisition copies of the Register of Births and Deaths and the admission register of any

educational institution in any area.[273] The complete electoral rolls – containing details such as full name, relatives, age, sex and EPIC number - are required by law to be available for inspection at office of the registration officer, and copies of the rolls must be supplied to every political party[274] All citizens may obtain copies of extracts of the rolls pertaining to themselves upon payment of a fee.[275] In addition, it has become common practice for state election commission websites to provide online access to complete lists of electoral rolls that they maintain.[276] Political parties are provided with soft copies of complete electoral rolls, although photographs of voters are not made available to them in soft copy.[277]

In August 1993, in what was probably the first initiative of its kind and scale, the ECI decided to issue Elector's Photo Identity Cards (EPIC) to all voters in the country to ensure their correct identification and prevent impersonation.[278] The EPIC contains the following details - the name of the elector, Relation's name, Date of Birth, Gender, Address and the photograph of the elector. In addition, every EPIC is fixed with a security hologram and has a unique 10 character alphanumeric string called the EPIC Number.[279]

Despite having the potential to serve as a kind of pan-Indian unique identification, in practice, the scheme was highly decentralized with databases being maintained at the level of each constituency instead of in one centralized repository. There was no standardization in either the database technology employed or data structure adopted at each level, and this led to

---

[273] REGISTRATION OF ELECTOR RULES, 1960, Rule 9 (1961), http://lawmin.nic.in/legislative/election/volume%202/registration%20of%20electors%20rules,%201960.pdf (last visited Oct 30, 2011).

[274] *Id.* at Rule 22.

[275] Copies of the rolls, including photo rolls, requisitioned by citizens under the Right to Information Act may be provided only if they do not deal with specific third-party individuals. I.e. it is possible to requisition, for instance page 45 of the Electoral rolls, but it is not possible to specifically requisition the portion of the rolls on which Prashant Iyengar's name appears. Hand Book for Electoral Registration Officers Election Commission of India 2008, 56 (2008), http://eci.nic.in/eci_main/ElectoralLaws/HandBooks/ERO_HANDBOOK.pdf (last visited Oct 30, 2011).

[276] *Id.* at 28.; Thiis appears to be a recent departure from a previous policy which absolutely forbade the disemination of electoral rolls on websites. *See ITEM NO. 154: Election Commission's letter No.485/Comp/16/99, dated 31.08.1999 addressed to the Chief Electoral Officers of All States/UTs*, *in* COMPENDIUM OF INSTRUCTIONS ON ELECTORAL ROLLS, EPIC, SLAS & COMPUTERISATION 821 (2006), http://eci.nic.in/eci_main/ElectoralLaws/HandBooks/Compendium_of_Instructions_on_ERs_EPIC_SLA_Computerisation.pdf (last visited Oct 31, 2011).

[277] Hand Book for Electoral Registration Officers Election Commission of India 2008, *supra* note___ at 13.

[278] REGISTRATION OF ELECTOR RULES, 1960, *supra* note___ at Rule 28.

[279] Ashish Chakraborty, RETENTION OF OLD EPIC NUMBERS FOR NEW/DUPLICATE EPICS AND MAINTENANCE AND UPKEEP OF PHOTO-ROLL IMAGE DATABASE. (2008), http://eci.nic.in/eci_main/eroll&epic/ins_180908.pdf (last visited Oct 30, 2011).

incompatible databases being maintained at each level.[280] The fact that databases were being maintained in regional languages made the task of integration even more difficult. Voters were required to obtain fresh ID cards in each new constituency that they shifted to, and inadequate co-ordination within the election commission led to a situation where it was possible for voters to maintain separate voter IDs in different constituencies that they transferred to. In addition, the database of voters and the database of photographs were frequently maintained separately and were imperfectly linked.

In order to streamline the process and consolidate the disaggregated data, in February 2008, the ECI decided to centralize its databases and directed the Electoral Database and the photo database to be centrally maintained in one database for the entire State.[281]

Without commenting on the prospects of this new centralized database, it would be pertinent to consider some aspects of the career of the voter ID card so far:

1. Firstly, like the Ration Card and the PAN Cards, Voter ID cards have proven highly susceptible to forgery. One source of these fakes is the pilferage of the 'security holograms' that have occurred from the offices of the election commission. In November 2003, the Madhya Pradesh state election commission had reportedly 'misplaced' over 5 lakh (500,000) of these holograms. Although most were subsequently recovered, there were no records indicating the actual numbers lost.[282] In August 2006, a leader of a political party in West Bengal was arrested "for running an offset press that printed fake

[280] The website of the Tamil Nadu Election Commission provides a brief, but interesting account of the challenges this lack of standardisation posed in subsequent attempts at consolidating the various databases. Databases that had been maintained since 1998 in MS Access format in a dated characterset (ISCII) had to be converted in 2008 to a more modern RDBMS in Unicode format. In addition the Table structure had to be altered according to a standardised structure that would enable transfer of information between the various election commission offices - a step which should have been taken at the outset. See *Database Management*, THE CHIEF ELECTORAL OFFICER OF TAMIL NADU, http://www.elections.tn.nic.in/database_management.htm (last visited Oct 30, 2011); A similar account also emerges from the experience of the State Election Commission in Goa when it migrated to a new database. *ECI votes for GEL's new electoral roll management software in Goa*, TIMES OF INDIA, January 2, 2011, http://articles.timesofindia.indiatimes.com/2011-01-02/goa/28360336_1_electoral-roll-mother-roll-summary-revision (last visited Oct 31, 2011).

[281] *Id.* at Para 5.

[282] Harosh Singh Bal, *50,000 struck off Mangawa rolls*, INDIAN EXPRESS, November 10, 2003, http://www.indianexpress.com/oldStory/35026/ (last visited Oct 31, 2011).

voter ID cards".[283] According to the news report, "he acquired a hologram software from Mumbai and used it to make dud voter ID cards. *Such machines can be easily procured from the nearby Nohata Market, close to the Benepole border*."[284]As recently as August 2011, the police arrested three members of a gang in Secunderabad who were issuing fake EPIC cards. The news report revealed that "Twenty-one EPICs, 400 holograms and stamps were seized from the arrested persons".[285] Previously similar incidents had been reported in New Delhi[286] and Bhubaneshwar[287]. Frequently the supply of the holograms to these forgers has been traced to personnel within the Election Commission itself indicating lax or missing security protocols within the organisation. In the Secunderabad case, newspapers reported that an attender in the Election Commission office, who was the main accused, had "secured an old software used to make the EPIC and stored it in his computer at home. Using this software, he would scan an EPIC, replace the details with those of his clients and issue the card using the holograms available with him."[288] In another incident in Kanpur, the accused were reportedly supported by government officials who actively provided them with details needed to prepare fake electoral IDs.[289]

2. In several cases of forgery, the mischief has been traced to the private company contracted by the Election Commission to record data and supply the electoral ID cards. In October 2007, for instance, the Maharashtra State Election Commission lodged an FIR against an employee of a private software company who admitted to running a fake voter ID scam.[290] In 2003, an employee of the private agency contracted to make ID cards in

---

[283] *Fake voter IDs: CPM leader held*, TIMES OF INDIA, January 20, 2006, http://articles.timesofindia.indiatimes.com/2006-01-20/india/27797681_1_fake-voter-voter-id-cards-cpm-leader (last visited Oct 31, 2011).
[284] *Id.*
[285] *Fake voter ID card racket busted*, THE HINDU, August 21, 2011, http://www.thehindu.com/todays-paper/tp-national/tp-andhrapradesh/article2378331.ece (last visited Oct 31, 2011).
[286] *Racket in voter I-cards busted, three arrested*, THE HINDU, January 29, 2003, http://www.hindu.com/2003/01/29/stories/2003012904690300.htm (last visited Oct 31, 2011).
[287] *Fake voter ID card racket busted*, WELCOMEORISSA.COM (2009), http://welcomeorissa.com/Fake+voter+ID+card+racket+busted-orissa_news-19784-24-04-2009.html (last visited Oct 31, 2011).
[288] Fake voter ID card racket busted, *supra* note___.
[289] *Fake voter ID card racket busted, three arrested*, INDIAN EXPRESS, April 15, 2009, http://www.indianexpress.com/news/fake-voter-id-card-racket-busted-three-arre/447106/ (last visited Oct 31, 2011).
[290] Kiran Tare & Prashant Hamine, *Voter card issuer flees, EC lodges FIR*, DNA INDIA, December 9, 2007, http://www.dnaindia.com/mumbai/report_voter-card-issuer-flees-ec-lodges-fir_1138132 (last visited Oct 31, 2011).

> Mahipalpur constituency was arrested for running a fake ID racket.[291] In the recent case in Secunderabad, mentioned above, the news report observed "The entry of data was assigned to the CMC Ltd. on contract basis but there were no records showing details of voters approved by the electoral officer to make entries in the database. "*This suggests that an employee of the private company can enter details of any person at his will and get a voter ID card issued*", the Inspector observed."[292] In this case, the police were reportedly investigating the role of the private agency. In another revealing incident, the Bangalore Municipal Corporation (BBMP), who had outsourced the task of data entry of voter ID cards on an ad hoc basis to unskilled and "unemployed youths" reportedly conceded that "BBMP is aware that *computers used in cyber cafes by unskilled youngsters have led to mistakes and leakage of data*, but such usage has become inevitable due to shortage of computers" (emphasis added) [293]

Despite the high incidence of fakes, the Voter ID card remains today one of the most widely used modes of identification used by citizens. An important source of concern from the privacy perspective is the degree to which the enrolment process is controlled by the contracted agency. Apart from thinly worded contractual terms which require the agency to turn over all data collected to the Election Commission and not retain anything beyond the period of the contract, there are usually no safeguards and standards that the ECI mandates these agencies to observe. Already, as witnessed above, this laxity has occasioned the mushrooming of fake voter id rackets. An important contribution to privacy, in this context, would be the evolution of a strong data protection guideline, backed with sanctions to govern those agencies whom the ECI contracts to perform the tasks of enrollment and issual of ID cards.

### 17.2.3 The National Population Register/ Multipurpose National Identity Cards (MNIC)/National ID Number

> The survey party distributed jute bags among the populace of Pooth Khurd, a village in Gurgaon. The bag has MNIC written in Hindi with the possible benefits that will accrue to the owner of the card enumerated below. M-N-I-C or the Multiple purpose National Identity Card, written as /BahuUddashaye Rashtriya Pechan Patra /and is being read as /Bahu Deshya Rashtriya Pechan Patra /or Multiple country National Identity Card. *A*

[291] Racket in voter I-cards busted, three arrested, *supra* note___.
[292] Fake voter ID card racket busted, *supra* note___.
[293] Sunitha Rao, *EPIC errors are coming out of cyber cafes as BBMP hires untrained youths to fill in data*, TIMES OF INDIA, October 7, 2011, http://goo.gl/5NOoC (last visited Oct 31, 2011).

> *farmer says that it was the SDM and the survey people who kept on saying that after the green [Hara] card or the MNIC, foreign travel will be easy and hassle free.* The desire for the 'Hara' card also hints towards a manifestation of dreams of mobility transcending political and geographical borders. (emphasis added)
>
> 'MNIC' Sarai, Information Society Log[294]

In 2004, the Citizenship Act 1955 was amended to include a new section dealing with the 'Issue of National Identity Cards'. The new Section 14A empowers the Government to "compulsorily register every citizen and issue a national identity card to him". The section designates the Registrar General of India – in charge of conducting the decennial Census in India – as the National Registration Authority for the purpose of enrolling citizens and issuing them with identity cards. Rules have been framed under the Act which make it mandatory for every Citizen of India to get themselves "registered in the Local Register of Indian Citizens during the period of initialization".[295] Failure to do so is punishable with a fine of up to Rs. 1000. Under the rules, National Identity cards are issued to every citizen enrolled in the National Register of Indian Citizens. The local registrar is empowered, upon an application from the citizen to make modifications in the register with respect to changes in name, residential address, marital status or change of sex.[296]

In 2010-2011, as a part of the decennial census, the actual process of compiling the National Population Register and issuing ID Cards was initiated. According to the website of the Registrar General, the "NPR will be a comprehensive identity database that would help in better targeting of the benefits and services under the Government schemes/programmes, improve planning and help strengthen security of the country. This is being done for the first time in the country."

The website also provides a short description of the process by which the registration would be carried out which is worth quoting in entirety:

> Details such as Name, Date of Birth, Sex, Present Address, Permanent Address, Names of Father, Mother and Spouse etc will be gathered by visiting each and every household. All usual residents will be eligible to be included irrespective of their Nationality. Each and every household will be given an Acknowledgement Slip at the time of enumeration.

[294] *MNIC*, SARAI , http://www.sarai.net/research/information-society/logs/mnic (last visited Nov 1, 2011).
[295] CITIZENSHIP (REGISTRATION OF CITIZENS AND ISSUE OF NATIONAL IDENTITY CARDS) RULES, CITIZENSHIP ACT, 1955 (2003), http://mha.nic.in/pdfs/citizenship_rules2003.pdf (last visited Nov 1, 2011). Curiously, these rules were issued *before* the insertion of Section 14A in the Citizenship Act, so the procedure for issue of Identity cards was specified prior to the power to issue them was granted by the legislature.
[296] *Id.* at Rule 12.

> The data will then be entered into computers in the local language of the State as well as in English. Once this database has been created, biometrics such as photograph, 10 fingerprints and probably Iris information will be added for all persons aged 15 years and above. This will be done by arranging camps at every village and at the ward level in every town. Each household will be required to bring the Acknowledgement Slip to such camps. Those who miss these camps will be given the opportunity to present themselves at permanent NPR Centres to be set up at the Tehsil/Town level. In the next step, data will be printed out and displayed at prominent places within the village and ward for the public to see. Objections will be sought and registered at this stage. Each of these objections will then be enquired into by the local Revenue Department Officer and a proper disposal given in writing. Persons aggrieved by such order have a right of appeal to the Tehsildar and then to the District Collector. Once this process is over, the lists will be placed in the Gram Sabha in villages and the Ward Committee in towns. Claims and Objections will be received at this stage also and dealt with in the same manner described above. The Gram Sabha/Ward Committee has to give its clearance or objection within a fixed period of time after which it will be deemed that the lists have been cleared. The lists thus authenticated will then be sent to the Unique Identity Authority of India (UIDAI) for de-duplication and issue of UID Numbers. All duplicates will be eliminated at this stage based on comparison of biometrics. Unique ID numbers will also be generated for every person. The cleaned database along with the UID Number will then be sent back to the Office of the Registrar General and Census Commissioner, India (ORG&CCI) and would form the National Population Register.

Under the scheme, the issue of the National Identity Cards is the last step and is to be "given in a phased manner to all usual residents" with no specific timeline set. In September 2011, a Public Interest Litigation was filed against the registrar general alleging that the machinery, which the government was about to procure for manufacturing the MNICs did not meet the specifications of the technical committee and would result in the issuing of cards which would "not survive more than two years"[297]

Apart from the technical problems, one source of concern for privacy advocates is that one major step in the process – digitization of NPR forms collected from individuals is being outsourced to private companies. More specifically, personnel from private companies such as ECIL are responsible for the digitization of all demographic data collected by the Census department. As witnessed above, in the context of the electoral id, this is a process fraught with the risk of data theft. In the absence of strict data protection guidelines on the protocol to be observed by these

[297] *HC notice to Centre on MNIC quality*, DECCAN HERALD, September 2, 2011, http://www.deccanherald.com/content/93537/hc-notice-centre-mnic-quality.html (last visited Nov 1, 2011).

personnel, the protection of citizens informational privacy hinges on the ability and willingness of the State to enforce contractual clauses against the agencies hired by it for this task.

### 17.2.4 The Unique Identity Scheme (Aadhar)

#### *17.2.4.1 A voluntary ID?*

The UID claims itself to be a voluntary scheme. However, owing to the complex operational structure that the UID Scheme adopts, the actual task of enrollment entirely in the hands of third party 'Registrars' who include a host of Central and State social security and welfare departments (including the Ministry of Rural Development which administers the Rural employment guarantee scheme), banks and insurance companies. There is nothing in the Aadhar Scheme that *forbids* these Registrars from making access to their services conditional on one's consent to UID registration. In practice, many of them have and will continue to make UID registration a preliminary formality before access is granted to their services. So the citizen's 'freedom' to resist UID registration depends on their ability to forego, say, minimum guarantee of the right to employment, cooking gas, banking and insurance services, food rations etc.

In addition, the Registrar General of India, the authority responsible for compiling the National Population Register of India under the Citizenship Act, also happens to be a 'Registrar' for the purposes of the UID. This means that one's registration in the NPR will entail automatic *enrollment* in the UID. The Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003 makes it mandatory for everyone to be enrolled in the National Population Register. So, paradoxically, although the Aadhar number does not confer citizenship, one cannot be a citizen anymore without owning an Aadhar number.

#### *17.2.4.2 Data Collection and the UID*

A frequently assertion about the UID scheme is that the data collected will be limited to a standard set of information like one's name, residence, date of birth, photo, all 10 finger prints and iris image. However, as mentioned previously, the entire process of enrollment is carried out through Registrars who have absolute freedom to expand the categories of information collected to include data that is entirely orthogonal to the purposes of the UID. This freedom is typically guaranteed by a clause in the MOUs which the UIDAI has signed with Registrars enabling them to collect additional data that "is required for their business or service". Thus, for instance, in

Himachal Pradesh, citizens are asked to provide additional details such as information about their ration cards, PAN cards, LPG connection and bank accounts[298]

#### *17.2.4.3 Privacy and the UID*

Although the UIDAI makes repeated assertions regarding its intent to respect privacy and ensure data protection, the precise mechanism through which these objectives will be secured is extremely unclear.

1. To begin with, the entire responsibility for devising schemes for safeguarding information during the collection phase rests entirely on the Registrars. The UIDAI's own responsibility for privacy begins only from the moment the information is transmitted to it by the Registrars – by which time the information has already passed through many hands including the Enrolling Agency, and the Intermediary who passes on information from the Registrar to the UIDAI.

2. Rather than setting out an explicit redressal mechanism and a liability regime for privacy violations, the UID's documents stop at loosely describing the responsibility of the Registrars as a 'fiduciary duty' towards the resident/citizen's information. The Registrars are tasked with maintaining records of the data collected for a minimum period of six months. No maximum period is specified and Registrars are free to make what use of the data they see fit.

3. In addition, the Registrars are mandated to keep copies of all documents collected from the Resident either in physical or scanned copies "till the UIDAI finalizes its document storage agency."[299]

4. The 'Data Protection and Security Guidelines' which the UIDAI requires all Registrars to observe merely contains pious injunctions calling on them to observe care at all stages of data collection and to develop appropriate internal policies. There is mention of the

[298] *UID project picks up pace*, INDIAN EXPRESS, January 11, 2011, http://www.indianexpress.com/story-print/735790 (last visited Jan 22, 2011).

[299] DOCUMENT STORAGE GUIDELINES V1.2 (2010), http://uidai.gov.in/images/FrontPageUpdates/ROB/D11%20Document%20Storage%20Guidelines%20for%20Registrars%20final%2005082010.pdf (last visited Oct 24, 2011).

desirability of external audits and periodic reporting mechanisms, but the details of these schemes are left to the individual Registrar to draw up.

5. Although the Draft National Identification Authority of India Bill penalizes the intentional disclosure or dissemination of identity information collected in the course of enrollment or authentication, this does not guard against accidental leaks and does not mandate the service providers to positively employ heightened security procedures. Prosecution of offences under the Act can only proceed with the sanction of the UID Authority, which further burdens the task of criminal enforcement in these cases and would make it difficult for individuals to obtain redress quickly. The total absence of a provision for civil remedies against Registrars makes it unlikely that they will take the task of protecting privacy seriously.

In other words, the individual's right to privacy is only as strong as the weakest link in the elaborate chain of information collection, processing and storage.

#### *17.2.4.4 Data Sharing and the UID*

The UID has frequently claimed that it would not disclose any information, but merely authenticate information with Yes/No answers. For instance, in April, 2010, in response to a question in the course of an interview, Nandan Nilekani said "UID itself has very limited fields, it has only four or five fields — name, address, date of birth, sex and all that. But it also does not supply this data to anybody. .. the only authentication you can get from our system is a yes or no. So, you can't query and say what's this guys name or what's his date of birth, you can't get all that [300]

This statement is, however misleading belied by many of the UIDAI's own documents.

1. The draft NIA Bill, for instance, permits the Authority to issue regulations on the sharing of "the information of aadhaar number holders, with their written consent, with such agencies engaged in delivery of public benefits and public services as the Authority may

[300] *To issue first set of UIDs by Feb 2011: Nilekani*, MONEY CONTROL, 2010, http://www.moneycontrol.com/news/business/to-issue-first-setuids-by-feb-2011-nilekani_449820-4.html (last visited Jan 22, 2011).

by order direct". In practice, prior "written consent" for sharing is obtained from the resident as a matter of course at the time of enrollment itself, and it is impossible to obtain an Aadhar number without consenting to sharing by the UID Authority.[301] In practice, in India, a large number of forms will be filled in by assistants and the written consent box will be ticked as a matter of course without the resident understanding the full implications of her "consent".

2. The draft NIA Bill permits the authority to "make any disclosure of information (including identity information) made in the interests of national security in pursuance of a direction to that effect issued by an officer not below the rank of Joint Secretary or equivalent in the Central Government after obtaining approval of the Minister in charge". There is nothing in the Act that requires that this information be made available on an individual basis – in other words, it is possible for the data to be shared en-masse with any agency "in the interests of national security".

3. There is nothing preventing "Registrars" who carry out the actual data collection functions from sharing this information with anyone they choose. Thus, for instance, the Aadhar information collected during the exercise of compiling the National Population Register will can be shared in whichever manner the Registrar General of India chooses – irrespective of what the UIDAI does with that information.

So, while *ordinarily*, the UIDAI would not authenticate information other than giving Yes/No responses, there are mechanisms already in place that presume that all this information will be made available, on demand, to whichever agency that happens to be interested.

In September 2011, the National Human Rights Commission, set up under the Human Rights Act, issued an opinion cautioning against the potential harms of the Aadhar scheme. The Commission noted the possible discriminatory effects of the scheme and the fact that no provision had been made in the Bill for compensation to the victim in case of breach. One newspaper account reported that "The NHRC noted that the "biometric information" and "demographic information" have not been clearly defined and while framing the regulations

[301] For instance, a flowchart of the Resident Enrollment Process issued by the UID stipulates "Record Resident's consent for Information Sharing" as the tenth step in the enrollment process. Unless this step is followed, the enrollment process cannot proceed!

under the Act, precautions should be taken to ensure that individuals are not required to disclose confidential information about themselves."[302]

- is there a national ID number, card, or other form of infrastructure? is there a Tax ID number and how is it used?

- is there a mandatory, legal, or de facto form of identification? what kind of information is linked to the record?

- are the identity systems 'electronic' or 'smart' with the use of digital data, smartcards, RFID?

## §18 Biometrics

- is there a national biometric system for fingerprints, iris or retinal scans, facial recognition?

- do government or other sectors collect biometric information?

## §19 Medical Privacy and Health Management

Under the Epidemic Diseases Act 1897, if a State Government is satisfied that the state is "visited by, or threatened with, an outbreak of any dangerous epidemic disease" then it may take measures to check the outbreak. Such measures may include "inspection of persons travelling by railway or otherwise, and the segregation, in hospital, temporary accommodation or otherwise, of persons suspected by the inspecting officer of being infected with any such disease." In 2009, the Act was invoked in the state of Maharashtra to combat Swine Flu. Rules were promulgated requiring anyone with swine flu symptoms to go to designated government hospitals and providing that severely affected would be quarantined. The rules allowed local councils to check students for signs of swine flu in schools.[303]

There is no uniform statute specifically protecting the privacy of health information in India. However doctors are required to maintain the confidentiality of their patients, and various

[302] *"Aadhaar" numbers could lead to discrimination: NHRC*, DECCAN HERALD, September 18, 2011, http://www.deccanherald.com/content/191739/aadhaar-numbers-could-lead-discrimination.html (last visited Oct 23, 2011).
[303] Steve Herman, *India Enacts New Guidelines After 1st Swine Flu Death*, VOICE OF AMERICA (August 2009), http://www.voanews.com/english/news/a-13-2009-08-04-voa11-68755652.html (last visited Oct 17, 2011).

regulations have been passed by the insurance regulator requiring a high level of confidentiality with respect to health insurance records. Each of these is examined in turn.

## 19.1 Privacy in the Medical Profession

In 2002, the Medical Council of India notified the Indian Medical Council (Professional conduct, Etiquette and Ethics) Regulations which contain ethical injunctions backed by disciplinary action in cases of breaches. Several of the articles in these regulations relate to privacy, for instance

- Every physician is required to maintain medical records pertaining to indoor patients for a period of 3 years from the date of commencement of the treatment. Upon request by the patients / authorised agents or legal authorities involved these documents should be issued within a period of 72 hours.

- Article 2.2 requires physicians to maintain Confidences concerning individual or domestic life entrusted by patients to a physician. Defects in the disposition or character of patients observed during medical attendance should never be revealed unless their revelation is required by the laws of the State. The rule also requires the physician, controversially to evaluate "whether his duty to society requires him to employ knowledge, obtained through confidence as a physician, to protect a healthy person against a communicable disease to which he is about to be exposed". In such an instance, the rules advice the physician to "act as he would wish another to act toward one of his own family in like circumstances."

- Article 7.14 enjoins the registered medical practitioner not to disclose the secrets of a patient that have been learnt in the exercise of his / her profession except –

    1. in a court of law under orders of the Presiding Judge;

    2. in circumstances where there is a serious and identified risk to a specific person and / or community; and

    3. notifiable diseases.

- Article 7.17 forbids a medical practitioner from publishing photographs or case reports of patients without their permission, in any medical or other journal in a manner by which

their identity could be made out. If the identity is not to be disclosed, however, the consent is not needed.

In one of the most important cases to have come up on the issue of privacy, a person sued a hospital for having disclosed his HIV status to his fiancé without his knowledge resulting in their wedding being called off. In *Mr. X vs Hospital Z*, 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. The Supreme Court while affirming the duty of confidentiality owed to patients, 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."

## 19.2 Privacy and Health Insurance Records

The Insurance Regulatory and Development Authority – the national regulator overseeing the insurance industry in India – has issued a number of guidelines which cumulatively promote privacy in the health insurance sector. Illustratively, guidelines have been issued regulating the use of telemarketing to solicit insurance business,[304] third party administrators, outsourcing of functions and health insurance portability which each contain measures designed to promote customer confidentiality and privacy.

### 19.2.1 Third Party Administrators Regulations

In 2001, the IRDA (Third Party Administrators - Health Services) Regulations[305] were issued which place restrictions on 'third party administrators' (TPAs) who provide 'health services' under agreement with insurance companies. TPAs are typically companies which provide information services like back-end processing of claims, processing cashless cards etc. Such TPAs must obtain a license from the IRDA[306] and must operate in accordance with a code of conduct which requires them, *inter alia*, to "refrain from trading on information and the records

[304] GUIDELINES ON DISTANCE MARKETING OF INSURANCE PRODUCTS, (2011), http://goo.gl/0KfFn (last visited Oct 15, 2011).The guidelines require that "No inconvenience, nuisance or harm shall be caused to the clients in the course of solicitation or thereafter. Full disclosures shall be made to the clients under all modes of distance marketing and the requirements of confidentiality, privacy and non-disclosure shall be complied with."[Item 9.3(iv)]

[305] The IRDA (Third Party Administrators - Health Services) Regulations 2001, (2001), http://www.irdaindia.org/tpareg.htm (last visited Oct 15, 2011).

[306] As of this writing there are 29 licensed TPAs in India. *See* List of TPAs Updated as on 3rd October, 2011, INSURANCE REGULATORY AND DEVELOPMENT AUTHORITY (2011), http://www.irda.gov.in/ADMINCMS/cms/NormalData_Layout.aspx?page=PageNo646 (last visited Oct 15, 2011).

of its business" and "maintain the confidentiality of the data collected by it in the course of its agreement". Regulation 22 of these regulations requires TPAs to "maintain proper records of all transactions carried out by it on behalf of an insurance company" and keep them "for a period of not less than three years". In maintaining the records, the TPAs are required to "follow strictly the professional confidentiality between the parties as required". However, this obligation "does not prevent the TPA from parting with the relevant information to any Court of Law/Tribunal, the Government, or the Authority in the case of any investigation carried out or proposed to be carried out by the Authority against the insurance company, TPA or any other person or for any other reason." If the TPA's license is revoked for any reason, then the "data collected by the TPA and all the books, records or documents, etc., relating to the business carried on by it with regard to an insurance company" is to be handed over to the insurance company by the TPA.

### 19.2.2 Sharing of Data Regulations

In 2010, in a somewhat ambivalent move, the IRDA issued regulations stipulating the conditions under which 'referral companies' could sell their customer databases to insurance companies to enable them to solicit business. On the one hand, these regulations - RDA (Sharing of Database for Distribution of Insurance Products) Regulations, 2010- are welcome, since they prescribe rigorous qualifications for referral companies from whom insurance companies may lawfully purchase databases. All previous referral arrangements that do not conform with the regulations are required to be terminated. This introduces an element of conservatism into the manner in which insurance companies are permitted to source their clients. On the flip side, however, the regulations lay the foundation for wholesale transfers of databases from government and public sector bodies to insurance companies.

The regulations place welcome restrictions on the kinds of entities that may be allowed to transfer their databases to insurance companies. Such 'referral companies' must, for instance, a) seek and obtain approval from the IRDA, b) meet rigorous financial norms to qualify, c) not be a company engaged in the business of "acquisition and sale of data", d) nor provide retail banking services or be linked in any way to the insurance business, and e) must not have an existing referral agreement with any other insurer. They must not earn more than 10% of their total income from the referral business. In addition, the regulations require the referral company not to be bound "by any confidentiality agreement in the matter of sharing the personal and financial

databases of its customers." Referral companies are barred from providing details of their customers without their prior consent, and are forbidden from providing "details of any person/firm/company with whom they have not had any recorded business transaction". All agreements between insurers and referral companies must be submitted to the IRDA for approval. These measures are welcome since they provide a degree of government oversight into the manner in which insurance companies source their information. By placing restrictions on the kinds of entities who may supply databases to insurance companies, the IRDA has forestalled the sourcing of personal information for the insurance business from becoming a full blown business.

The less savory aspect of this regulation is that it seems to legalize the encourage the trade of databases of personal information from the government – who meet all the qualifications of a referral company - to insurance companies. In a report published in a prominent newspaper[307], a senior IRDA official reportedly said "Both state and central agencies have huge databases, not only in the urban and semi-urban areas but also in rural India. For example, it will be a coup if a health insurer can tie up with a government agency, such as a state hospital"". The same article quotes the MD of a private insurance company as saying that, "Organisations such as BSNL, MTNL and even Railways have a huge customer base. So far, we've not entered into agreement with any such agency but we may explore this opportunity".[308]

So although comforting in some respects, these regulations also have disconcerting implications for the future. It remains to be seen to what extent government databases are in fact transacted upon by virtue of these regulations.

### 19.2.3 Outsourcing Regulations

In February 2011, the IRDA issued guidelines permitting insurance companies to outsource their non-core functions including a range of data entry, telemarketing, receiving complaints and other functions.[309] The guidelines require the insurer to "take appropriate steps to require that third

[307] Dheeraj Tiwari, *PSUs may open databases for insurers in referral plan*, ECONOMIC TIMES, July 14, 2010, http://articles.economictimes.indiatimes.com/2010-07-14/news/28416436_1_referral-insurance-regulator-insurance-companies (last visited Oct 15, 2011).
[308] *Ibid*
[309] GUIDELINES ON OUTSOURCING OF ACTIVITIES BY INSURANCE COMPANIES, (2011), http://goo.gl/fUBvP (last visited Oct 15, 2011).

party service providers protect confidential information of both the Insurer and its clients from intentional or inadvertent disclosure to unauthorized persons"[310].

## 19.3 National Health Records

Although India does not currently have a national health record system, such a system is very likely to take shape under Health Insurance Portability guidelines issued by the IRDA as well as the Rashtriya Swasthya Bima Yojana (RSBY) – the National Health Insurance Scheme.

### 19.3.1 Health Insurance Portability Regulations

In February 2011, with a view to promoting competition in health insurance services, issued a circular on Health Insurance portability. The guidelines direct all health insurers "that the entire database including the claim details of the policies, where the policyholders has opted for portability, shall be shared with their counterparts, if requested by the counterpart within seven working days of such request by the counterpart".[311] Pursuant to these guidelines, in June 2011, the IRDA issued a press release announcing the setting up, by October 2011, of a database to facilitate health insurance portability between different companies[312]. In September 2011, comprehensive guidelines were issued on Health Insurance portability according to which insurance companies would be provided a web-based facility created by the Authority to input all relevant details on health insurance policies issued by them to individuals who wish to move to another company. These details would then be accessible by the new insurer. As of this writing, however, this web-based interface has not yet been launched.

### 19.3.2 The National Health Insurance Scheme

The RSBY was launched in 2008 by the Ministry of Labour and Employment, Government of India to provide health insurance coverage for Below Poverty Line (BPL) families. The objective of RSBY is to provide protection to BPL households from financial liabilities arising out of health shocks that involve hospitalization. Beneficiaries under RSBY are entitled to

---

[310] *Ibid*

[311] Chairman, IRDA, PORTABILITY OF HEALTH INSURANCE POLICIES (2011), http://goo.gl/Gxlko (last visited Oct 15, 2011).

[312] PRESS RELEASE:PORTABILITY OF HEALTH INSURANCE, (2011), http://www.irda.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo1316&flag=1&mid=Press%20releases (last visited Oct 15, 2011).

hospitalization coverage up to Rs. 30,000/- for most of the diseases that require hospitalization. The Scheme aims to enroll up to 300 million Indians by 2012. [313]

One of the hallmarks of the scheme is its heavy reliance on smart cards to ensure delivery of services. The website of the scheme claims that currently, as many as 25 million smart cards have been issued to beneficiaries. Under the scheme, each state selects an insurance company to fulfill the mandate of the scheme within the territory of the state. The insurance company in turn enters into agreements with hospitals which will be the sites of service delivery. The state supplies the insurance company with a full list of BPL households enumerated according to the previous census.[314] It is the insurance company which is responsible for enrolling beneficiaries by obtaining their biometric data (fingerprints and photographs) and issuing them a smart card. Currently, the various insurance companies in each state have their own software and databases. According to one account, "A central server has been established wherein participating insurers (or TPAs on behalf of insurer) push/upload data in batches. Original bio-metric data containing finger prints, photographs etc is submitted in CD/hard disk separately".[315] However owing to inconsistencies in storage formats between insurers, a Central Data Management Agency is envisaged which would consolidate the data held by the various insurers and be "a comprehensive, uniform system" to operate the scheme.[316] Once installed, this CDMA would have the potential to become a National Health Record system.

## §20 Data Sharing

There are no laws forbidding data sharing either amongst government departments or between the government on the one hand and private agencies on the other. In some cases, for instance, in insurance, regulations affirmatively provide for the organized sharing of databases between the government and insurance companies. (See Section 18.2.2 of this report) In other cases such as e-passports and driving licenses, the government has entered into contracts with private

[313] *About the Scheme*, RASHTRIYA SWASTHYA BIMA YOJANA (2009), http://www.rsby.gov.in/about_rsby.html (last visited Oct 15, 2011).
[314] It is unclear to what extent this transfer is legal .
[315] Malti Jaiswal, *Insuring Health of Millions*, 8 IRDA JOURNAL 25-28 (2010), http://goo.gl/r5wmV (last visited Oct 16, 2011).
[316] Central Data Management Agency Concept Note, (2010), http://www.rsby.gov.in/Documents.aspx?ID=16 (last visited Oct 16, 2011).

companies to deliver electronic services which involve transactions on vast amounts of personal information.

## 20.1 Sharing data with the Government

Under the Income tax Act, tax authorities are permitted to obtain information from a range of agencies "such as banks, mutual funds, credit card companies — if they need it for any inquiry or proceedings…For instance, banks can be asked to provide details of their customers with cash deposits of over Rs 1 lakh. Credit card companies can be directed to furnish details about anyone who holds a card, irrespective of the value of purchases. Mutual funds have to give names and addresses of those who invest over Rs 1 lakh, when called for."[317]

In February 2011, the Securities Exchange Board of India (SEBI), in collaboration with the ministry of corporate affairs, and the Reserve Bank of India (RBI) proposed a format known as eXtensible business reporting language (XBRL) to be used by companies to report their financial details. Although not immediately applicable, the format is expected to enhance corporate surveillance by providing for cross-validation of data by different government departments.[318]

In addition, a number of policies have been drafted by the central government which provide for data sharing in some form. In this section we look at a few of the more important policies drafted in recent times.

## 20.2 Data Sharing by the Government

As noted above, over the past decade the state has been entering into contracts with private companies to provide electronic services and back-end processing which typically involves extensive sharing of personal information about citizens between the government and these private companies. Regardless of the existence of any articulated policy thrust towards data sharing, the Indian state has been in the *practice* of data sharing for at least a decade.

---

[317] Hema Ramakrishnan, *I-T likely to raise data-sharing , MFs on high-value deals*, ECONOMIC TIMES, August 7, 2006, http://articles.economictimes.indiatimes.com/2006-08-07/news/27447713_1_income-tax-tax-authorities-cib (last visited Oct 17, 2011).

[318] *Sebi proposes XBRL reporting system for mutual funds*, LIVEMINT, February 15, 2011, http://www.livemint.com/2011/02/15164528/Sebi-proposes-XBRL-reporting-s.html (last visited Oct 17, 2011); Souvit Sanyal, *New financial reporting format to enable data sharing among company watchdogs*, ECONOMIC TIMES, May 21, 2011, http://articles.economictimes.indiatimes.com/2011-05-21/news/29568795_1_xbrl-regulators-corporate-affairs (last visited Oct 17, 2011).

To quote just three examples: in October 2008, Tata Consultancy Services a prominent software services company in India was awarded a Rupees 1000 crore project to "provide passport-related services to Indian citizens in a speedy, convenient and transparent manner." In the absence of anything in the Passport Act prohibiting such wholesale outsourcing of essential functions, the task of safeguarding of citizens' privacy falls to the domain of contract law – assuming the contract between the state and the company contained a standard confidentiality clause - and the limited provisions of the IT Act dealing with data protection. (see infra) The contractual option can scarcely be regarded as a reliable privacy safeguard since it is only enforceable by the state against the private company and the state has had, at best, a patchy record has of defending its contractual rights against private companies.

The following extract, from a newspaper account about the outsourcing of biometric data collection illustrates the fluidity with which data sharing across databases occurs today between governments and contracted companies.

> "The project, conceived by WFP in 2007, was started a year ago with Hyderabad-based 4G Identity Solutions Pvt. Ltd as technology partner. Using its 125-member team, *the firm digitized old ration card registers and mapped these with the database of the 1997 BPL survey and 2002 household survey*. *The gram panchayat target beneficiary database was then transferred to some 6,000 enrolment stations in 2,445 villages, 41 wards and three urban local bodies where people queued up to get their biographic and biometric data recorded. Data from enrolment stations were sent to the 4G data centre for aggregation where de-duplication was done using a multi-modal biometric engine to check for fake enrolments. A final database of unique card holders was generated and stored in a centralised citizen database*. Rural households have been given laminated bar-coded ration cards and coupons since point-of-sale machines cannot be used in villages, several still without electricity." (emphasis mine)
>
> Indian Express, August 2003[319]

In this single paragraph, entire databases of citizens travel no less than 4 times (giving, perhaps, the company the eponymous title of '4G') and are mapped freely onto other databases created for other purposes. No law regulates these transfers – certainly nothing requires the prior consent of these citizens who have been mapped multiple times. One may conjecture that the company in question would be bound by normal contractual clauses of confidentiality – but this creates no

[319] Mohanty, *supra* note___.

obligations towards the citizens, none at any rate which citizens harmed by this move may enforce themselves. There is a prevailing sense that databases of information, once collected by the state, become the state's property through perhaps a variant of the 'eminent domain' theory applied to the realm of personal information.

In addition, the UID scheme discussed previously in this report expressly contemplates the sharing of information seamlessly across databases between a range of government agencies and private service providers. Although the draft UID bill does make a token reference to privacy, it seems a rather frail protection against the pernicious harms that could result from any data loss.

## 20.3 Data Sharing Policies

Alongside its many practices of data sharing, the Indian state has also issued several policy documents which expressly or impliedly encourage data sharing. Typically these are contained as injunctions in 'Information Technology' or 'E-Governance policies' issued periodically by the Central or State Governments. In this section we examine a few of these policy documents insofar as they pertain to data sharing by the Government.

### 20.3.1 National E-Governance Plan

In May 2006, the Indian government approved the National E-Governance Plan (NeGP), which was conceptualized as a holistic approach towards making government services available to people in their localities through CSCs while meeting goals of efficiency, transparency, reliability, and affordability. he plan includes proposals for "streamlining, aligning, optimizing and automating all internal processes across government boundaries"; with respect to courts, "online availability of judgments and cause list, e-filing of cases and notifications through e-mails"; and a portal providing "one-stop access to government services." The NeGP also lays the groundwork statewide area networks and data centers, and calls for research into "e-Government Enterprise Architecture Frameworks, Information Security, Data and Metadata Standards," among other areas. Most importantly, probably, the plan calls for "establishing 100,000 broadband Internet enabled Common Service Centers (CSCs) in rural areas of the country."[320]

[320] This text and the text from select subsequent sections has been adapted from a previous report authored by the Center for Internet and Society GLOVER WRIGHT, PRANESH PRAKASH & SUNIL ABRAHAM, REPORT ON OPEN GOVERNMENT DATA IN INDIA 25 (2011), http://www.cis-india.org/openness/publications/open-government.pdf (last visited Oct 17, 2011).

### 20.3.2 National Knowledge Commission recommendations[321]

In June 2005, Prime Minister Manmohan Singh constituted the National Knowledge Commission, an advisory body to the Office of the Prime Minister, (NKC) with the mandate to recommend policy reforms in the areas of "access to knowledge, creation and preservation of knowledge systems, [and] dissemination of knowledge and better knowledge services." The NKC was given a period of three years to conduct research and develop recommendations, which it issued in a series of reports now compiled in the "National Knowledge Commission Final Report 2006-2009." In its Final Report, the NKC made two recommendations particularly relevant to implementing an open government data in India. First, the NKC "recommended the establishment of a high-end National Knowledge Network connecting all … knowledge institutions in various fields and at various locations throughout the country, through an electronic digital broadband network with gigabit capacity". Second, and more relevant to considerations for open government data specifically, the NKC proposed that the government create a series of "national web based portals on certain key sectors such as Water, Energy, Environment, Teachers, Biodiversity, Health, Agriculture, Employment, Citizens Rights etc. [serving] as a single window for information on the given sector for all stakeholders and ... managed by a consortium consisting of representatives from a wide range of stakeholders". The NKC recommended that "[a]ll government departments should easily make available data sets they have, in a digital format to the portal consortium." It is unclear to what extent this recommendation has been followed. The NKC recognized that "data that is traditionally collected and managed separately, unrelated to each other, should now be seen together. But it indicated that "[t]here are no platforms or mechanisms currently in place to allow this to be done easily" and recommended also the development of clear guidelines for appropriate data formats as well as the regular updating of hosted data.

### 20.3.3 Public Information Infrastructure[322]

In 2009, Prime Minister Manmohan Singh appointed Sam Pitroda to the cabinet-level position of Adviser to the Prime Minister for Public Information Infrastructure and Innovations, tasked with developing a unified policy for information standards and practices incorporating both intra-government affairs and citizens' services.

---

[321] *Id.* at 27–28.
[322] *Id.* at 28–29.

In June 2010, Mr. Pitroda's office uploaded online a slide presentation on "Strengthening Democracy and Governance: Public Information Infrastructure." The presentation provides a basic overview of his proposal for a robust information system implicating all levels of government but focusing access and delivery on the level of the panchayat, or village assembly, which it specifies as the nodal point for citizen services

Included in the scheme is a national repository of information on people, including citizenship, resident, and household data; places, including villages, towns, streets, schools, hospitals, government offices, factories, officers, residences, stations, mines, minerals, dams, plants, rivers, parks, forests, farms, etc.; and programs and other government offices, such as the National Rural Employment Guarantee Scheme, the Public Distribution System, girl child benefit schemes, pensions, the judiciary, police and prisons, treasuries, land records, universalization of elementary education, and the National Rural Health mission, among others.

Applications hosted on the PII will include a shared Geographic Information System (GIS) for the Survey of India; the National Disaster Management program; the Urban Ministry; the Depart-ments of Space, Security, Environment, Health, and Rural Development; the Planning Commission; as well as private enterprises. Data from these entities will be publicly available on a single portal accessible by a variety of clients, including PCs and mobile phones. The portal will also incorporate applications, communities, mash-ups, and allow for a variety of analyses on data including including survey, remote sensing data, census, education, and health data, as well as forest, land use and groundwater data.

### 20.3.4 National Data Sharing and Accessibility Plan (NDSAP)

The National Data Sharing and Accessibility Policy (NDSAP) released in draft form in May 2011 under the Department of Science and Technology aims to set up a framework that would create a DATA.GOV.IN portal to release all non-classified data that is publicly held by various government departments.

Once finalized, under the policy, each department will have to provide a list of un-shareable items that will be determined using the provisions in the RTI Act and a hypothetical Privacy Act. Then all other data sets will be considered safe to be opened to the public.

MetaData would also be provided which would allow people to know what data is available. A three pronged classification system would be created to deal with different types of data; Open Access, Registered Access, and Restricted. A data warehouse will be set up to house current and historical data so that this information in is one place. [323]

The policy defines sensitive personal information as including "information collected, received, stored, transmitted or processed by body corporate or intermediary or any person, consisting of

- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.
- information related to financial information such as Bank account/credit card/debit card/other payment instrument details of the users
- physiological and me ntal health condition
- Medical records and history
- Biometric information
- information received by body corporate for processing, stored or processed under lawful contract or otherwise

It is still unclear what the future of this policy is. In June 2011, the government announced the imminent inauguration of a national government data portal. According to a newspaper account "All public data-from that on glacier meltdowns to monsoon charts to benami land--will be freely available at the click of a mouse with the launch of a national data portal next month."[324]

As of this writing, however, the NDSAP has not been approved by the Cabinet and no such portal is in existence.

- does the government share personal information with other governments?

[323] *Id.* at 30.
[324] *New Govt portal Data.Gov.In launch next month to ease information search*, ECONOMIC TIMES, June 4, 2011, http://articles.economictimes.indiatimes.com/2011-06-04/news/29620789_1_national-data-spatial-data-access (last visited Oct 17, 2011).

# §21 Protection of Privacy

## 21.1 Other Databases

In 2009, the Government announced the setting up of a "National Intelligence Grid" (NATGRID), reportedly modeled on the US intelligence Bureau model. The project is expected to consolidate "over 20 diversified databases such as banks, financial intermediaries, telecom service providers, etc". It is anticipated that "once institutionalized, it will promote effective and speedy retrieval of financial and non-financial data by over 10 government agencies (including RAW, Intelligence Bureau, Revenue Intelligence & the Income-tax department)".[325]

In July 2011, the Chennai police announced field trials for "the Crime Criminal Tracking Network and System (CCTNS), which would connect all the 1,400-odd police stations in the State to a central database". "Once operational", the report goes on to state, "the database would provide details of all first information reports (FIRs), pending cases and those relating to court proceedings."[326]

- are there other key databases of personal information worth noting?

- what regulatory regime governs the collection of information into databases?

## 21.2 Workplace Monitoring

Perhaps one of the most neglected areas of privacy law in India pertains to privacy at the workplace. Labour law in India has largely tended to focus on providing the organized sector with safe working environments and assuring workers a minimum and non-discriminatory wage. Perhaps the only privacy-type concern that is consistently referenced in these legislations has been the imperative to provide adequate toilet facilities to workmen at sites of employment.[327]

There is no law in India governing the extent to which employers are allowed to monitor their employees. In many industries such as call centers and IT enabled services, pervasive video surveillance of the workplace, use of biometric identity cards, monitoring of employee use of the

[325] Mukesh Butani, *UN convention to boost anti-corruption measures*, BUSINESS STANDARD, May 23, 2011, http://www.business-standard.com/india/news/un-convention-to-boost-anti-corruption-measures/436443/ (last visited Oct 24, 2011).
[326] Ajai Sreevatsan, *Citizen-friendly measures in crime tracking system*, THE HINDU, July 3, 2011, http://www.thehindu.com/news/cities/Chennai/article2153974.ece (last visited Jul 8, 2011).
[327] For Eg. See Section 42 of the Factories Act which requires that adequate 'washing facilities' be made available in every factory with separate facilities for male and female workers.

internet etc. is routine. Courts have not, so far dealt with this issue in a general way, perhaps because the legal framework to bring such an issue does not exist. For such an issue to arise before a court it would require a workman who has been dismissed or suspended to bring a suit claiming that employee surveillance was unfair and that he had been dismissed on account of it. Although the Constitution provides, as a Directive Principle of State Policy that the State shall endeavor to secure 'just and humane' conditions of work[328], there is currently no law that gives workmen a general remedy for 'unjust or inhumane conditions' of work. Employers are required minimally, to ensure that they do not expose employees to hazardous work conditions, provide basic sanitation and rest facilities, and are required to treat male and female employees equally. They may not dismiss their employees capriciously. Beyond that, however employers are accorded sovereignty over their workplace which may extend to surveilling their employees at will. Of course this may not extend to taking clandestine pictures of 'private areas' as forbidden by Section 66E of the Information Technology Act

Notwithstanding the thin articulation of workplace privacy rights in India, the Supreme Court has, in at least one case, placed fetters on the kind of information that employers could seek from employees. In *Mrs. Neera Mathur v Life Insurance Corporation*[329], the petitioner was a woman who had applied for a post in the Life Insurance Corporation of India. Having succeeded at a written test and interview she was asked to file a 'declaration form' and was also examined by a lady doctor on the panel of a corporation. Thereafter she was given a letter of appointment subject to a 6 month probation period. Shortly after her appointment, within her probation period, she applied for and took maternity leave for a period of three months. During this period, the company discharged her from service without assigning a reason. In a petition that ended up in the Supreme Court, the company defended its action on the ground that "the petitioner had deliberately withheld to mention the fact of being in the family way at the time of filling up the declaration form before medical examination for fitness". The declaration form contained several questions which impinged on her privacy including whether she was married, whether her menstrual periods always been regular and painless, the number of conceptions that had taken

[328] Article 42 of the Constitution of India

[329] Mrs. Neera Mathur v Life Insurance Corporation, AIR 1992 SC 392 (1991), http://www.indiankanoon.org/doc/832598/ (last visited Oct 10, 2011). *See* also V.S. Elizabeth, *Labour and fundamental human rights : Is discrimination law doing the job it is supposed to do?*, (2010), http://www.ialsnet.org/meetings/labour/papers/Elizabeth-India.pdf (last visited Oct 10, 2011).

place and the number that had gone to full term, the date of her last menstruation, the date of her last delivery and whether she had undergone an abortion. The Supreme Court held that the "real mischief" in this case was "the nature of the declaration required from a lady candidate". The court held that the details sought in the declaration form were "embarrassing if not humiliating" and that the "modesty and self respect" of a woman would "preclude the disclosure of such personal problems". The court ordered the company to reinstate the petitioner with full back wages and instructed the company to delete the offending columns in the declaration.

In the same vein, in a number of cases, courts have forbidden public sector employers in India from conducting HIV/AIDS tests without the consent of the employee or discriminating against HIV positive employees. In a celebrated case, MX v. ZY[330], a casual labourer, was tested for HIV by his employer, a public sector corporation. When he tested positive, though otherwise fit for his job, he was refused regularisation, and his contract was terminated. The court ruled that:

> " A government/public sector employer cannot deny employment or terminate the services of an HIV-positive employee solely because of his/her HIV-positive status, and any act of discrimination towards an employee on the basis of HIV-positive status is a violation of fundamental rights.
>
> An HIV-positive employee's services can only be terminated if a substantial risk of transmission is posed to co-employees or if she/he is unfit or unable to perform the essential functions of the job. Determining whether a person is unfit or incapable of performing the job depends on an individual inquiry (beyond a mere diagnostic test) into each specific case."[331]

There appears to be a strong line of rulings protecting persons with HIV from discrimination in public sector employment,[332] although private sector discrimination continues unchecked.

---

[330] AIR 1997 Bom 406

[331] Kajal Bharadwaj, DO WE NEED A SEPARATE LAW ON HIV/AIDS? INFOCHANGE INDIA (2008), http://infochangeindia.org/agenda/hiv/aids-big-questions/do-we-need-a-separate-law-on-hiv/aids.html (last visited Oct 15, 2011).

[332] Kajal Bharadwaj & Atiya Bose, LEGAL ISSUES THAT ARISE IN THE HIV CONTEXT HIV AIDS ONLINE (2008), http://www.hivaidsonline.in/index.php/HIV-Human-Rights/legal-issues-that-arise-in-the-hiv-context.html (last visited Oct 15, 2011).

## 21.3 Financial Privacy

Various laws require banks in India to maintain secrecy in relation to their client data. The following paragraphs provide brief details about these laws.

### 21.3.1 Customary/Statutory Banking Law

Both in banking customs[333] as well as statutes, there is a standardized, recognized obligation of secrecy. The wording in the following section is reproduced identically in many banking related acts including: SBI Act, 1955 – Section 44, SBI (Acquisition and Transfer of Undertakings) 1980 – Section 13, Credit Information Companies Act 2005 -section 29, and The Public Financial Institutions Act, 1983 -section 3. The section is applicable to the respective Bank as a whole and its directors, local boards, auditors, advisers, officers or other employees of the State Bank, and creditors are required in addition to affirm an oath of secrecy as provided. .

> Section 44.Obligation as to fidelity and secrecy.
>
> Obligation as to fidelity and secrecy.- (1) The State Bank shall observe, except as otherwise required by law, the practices and usages customary among bankers, and, in particular, it shall not divulge any information relating to or to the affairs of its constituents except in circumstances in which it is, in accordance with the law or practice and usage customary among bankers, necessary or appropriate for the State Bank to divulge such information.
>
> (2) Every director, member of a Local Board or of a Local Committee, auditor, adviser, officer or other employee of the State Bank shall, before entering upon his duties, make a declaration of fidelity and secrecy as in the form set out in the Second Schedule.

In *Shankarlal Agarwalla v. State Bank of India*, AIR 1987 Cal 29, a customer owned 261 bank currency notes of Rs. l.000/-each. Following the demonitisation of high value currency notes in 1978, he tendered these notes to the bank along with the requisite declaration and instricted the bank to credit his Current Account with the amount. The bank made declaration made by the

[333] One of the landmark cases on banking customs related to secrecy is the Court of Appeal case of Tournier v. National Provincial and Union Bank of England decided in 1924. The court upheld the general duty of secrecy arising out of a contract between the banker and the customer and held that the breach of it may give rise to a claim for substantial damages if injury has resulted from the breach. It is, however, not an absolute duty but qualified and is subject to certain reasonable exceptions. These exceptions have been incorporated into Indian law (see the Shankarlal Agarwalla case below)

customer available to the Income-tax Department who issued a notice under Sec. 226(3) of the Income-tax Act, attaching the said sum. Later the sum was released. The Calcutta High Court observed that among the duties of the banker towards the customer was the duty of secrecy. Such duty is a legal one arising out of the contract and was not merely a moral one. Breach of it could, therefore, give a claim for nominal damages or for substantial damages if injury is resulted from the breach. It was, however, not an absolute duty. but was a qualified one subject to certain exceptions. The instances being (l)the duty to obey an order under the Bankers' Books Evidence Act. (2) cases where a higher duty than the private duty is involved, as where danger to the State or public duty may supersede the duty of the agent to his principal, (3) of a bank issuing a writ claiming payment of an overdraft, stating on the face the amount of overdraft, and (4) the familiar case where the customer authorises a reference to his banker. The learned Judge further observed that the State Bank of India was directed by the Reserve Bank of India and the Ministry of Finance to furnish all particulars regarding deposit of bank notes to the Income-tax Department as soon as such notices were received. This instance had, therefore, come within the exceptions,

The recent Payment and Settlement Systems Act , 2007 imposes privacy obligations on those who manage online payment and settlement systems such as RTGS/NEFT etc. Section 22 of the Act enjoins “system providers” not to disclose the existence or contents of any document or part of any information given to him by a system participant, except where disclosure is

a) required under the provisions of this Act

b) made with the express or implied consent of the system participant concerned

c) in obedience to the orders passed by a court of competent jurisdiction

d) in obedience of a statutory authority in exercise of the powers conferred by a statute.

### 21.3.2 Reserve Bank of India regulations

The Reserve Bank of India has periodically issued guidelines, regulations and circulars which require banks to maintain the confidentiality and privacy of customers.

Thus, the Master Circular on Credit Card Operations of banks issued by the RBI in July 2010 contains an elaborate set of provisions on “Right to Privacy” and “Customer Confidentiality” under a section titled ‘Protection of Customer Rights’. The provisions inter alia, forbid the banks from making unsolicited calls, delivering unsolicited credit cards and from disclosing customer information to any third party without specific consent.

Similarly, the Master Circular on Customer Service in banks issued in 2009 contains a detailed clause on Customer Confidentiality Obligations. The clause reaffirms the customary banking obligation of secrecy and extends it by forbidding the usage of customer information for “cross-selling purposes”. It imposes a restriction on data collection by requiring Banks to “ensure that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard”.

In 2006, the Reserve Bank of India along with several banks of the Indian Banks Association (IBA) established a body called the Banking Codes and Standards Board of India to evolve a set of voluntary norms which banks would enforce on their own. A number of guidelines and notices have been produced by the BCSBI including the “Code of Bank's Commitment to Customers” which most banks in India adhere to. Enforcement is through a seriece of internal Grievance redressal mechanisms within each bank including a designated “Code Compliance Officer” and an Ombudsman.

Though these guidelines do provide differing and useful degrees of security and privacy, the lack of legislative oversight and enforcement allows the standards to be applied per institution and per-contract and enforcement is not guaranteed through parliamentary sanctions.

### 21.3.3 Data protection in the banking sector

Banks are governed by the Information Technology Act 2000 as amended in 2008. The latter amendments contain provisions that enjoin inter alia, banks to adopt reasonable security practices with respect to their databases. Customers of banks can, under the IT Act, obtain compensatory relief for losses arising out of data leakages as well as unauthorised disclosure of information by the banks for gain.

- what information are banks required to collect on their customers, e.g. are there 'Know Your Customer' rules?

- are there requirements for banks and financial institutions to disclose information to government agencies for suspicious transaction reporting?

- under what circumstances can government agencies gain access to financial information?

## 21.4 Consumer Privacy

Broadly, there are four potential avenues for the protection of consumer privacy in India.

Firstly, individual organizations may voluntarily commit to protect the information of their clients through “Privacy Policies” These become a component of the contractual commitments between the service providers and customers and are enforced through ordinary civil litigation.

Secondly, certain professions and industries have codes of privacy that they must statutorily abide by. This is true of such professions as the medical profession and the legal profession in India and the entire banking industry and the telecom industry. Rigorous privacy norms are set for each of these industries by their respective apex governing bodies. Penalties for breach include derecognition from the professional association and monetary penalties.

Thirdly, consumer privacy may be enforced by the specialized Consumer Dispute Tribunals under the Consumer Protection Act in India.

Lastly, the newly amended Information Technology Act imposes an obligation on anyone controlling data to indemnify against losses caused by the leakage/improper use of that data. This has already been discussed in preceding sections of this report.

In the following sections we look briefly in turn at the first three redressal options for consumers

### 21.4.1 Privacy Policies:

Several Indian companies have publicly stated privacy policies that they display on their website. We have profiled the privacy policies of two such companies as a sample.

**Airtel:** Defines personal information, informs users how their information will be used, describes which third parties will have access to your information, provides the ability to opt-out of commercial SMSs, provides an email address for privacy concerns.

**Rediff:** Provides email for customer support, states what personal information is collected from you, what information is collected from you by cookies, what information is collected about you and stored, who will collect the information about you, how the information will be used to advertise to you and tailor to your preferences, states the rights that advertisers have to your information, disclaimer of responsibility for any other websites linked to the page, states that the information released in a chat room is considered public information, defines third party usage, defines security measures taken, lays out what choices the consumer has regarding collection and distribution of their information, contains opt-out clauses, defines personal information, defines cookies, explains that consumers have the ability to correct inaccurate information, requires youth consent

To an extent, these privacy policies have been given additional legal sanction by the Intermediary Due Diligence Rules notified under the Information Technology Act which requires all data collectors to formulate and advertise such privacy policies. Redressal for violation of these privacy policies may be obtained following the procedure under the IT Act or through civil courts.

### 21.4.2 Professional/Industrial Regulations

As mentioned above, several professional bodies have privacy guidelines which their members must abide by.

#### *21.4.2.1 Advocates*

Rules of Professional Conduct have been framed under the Advocates Act and establish a code of conduct to be followed by lawyers in order to protect the confidence, information, and data of a client. It is important to note that the obligation of confidentiality continues even after the client relationship is terminated. The Evidence Act further buttresses the confidentiality of clients by making information passed between lawyer and client subject to a special privilege.

Complaints of ‘professional misconduct’ against advocates are referred to a Disciplinary Committee constituted under Section 36B of the Advocates Act, 1961 which is empowered to

impose a range of sanctions from censure to suspension to striking the advocate off the rolls of the bar council.

#### *21.4.2.2 Medical Practitioners*

Similarly, in 2002, the Medical Council of India notified the Indian Medical Council (Professional conduct, Etiquette and Ethics) Regulations which contain ethical injunctions backed by disciplinary action in cases of breaches. Several of these relate to privacy and have been discussed previously in this report in the context of medical privacy. (see *supra*)

#### *21.4.2.3 Banking and Telecom Industry*

The Banking and Telecom industry each have regulatory authorities which have periodically issued guidelines seeking to protect the privacy of customers. Thus, for instance, RBI's Customer Service statement obliges bankers to maintain secrecy, and not to divulge any information to third parties. Likewise, the TRAI has issued regulations on unsolicited commercial communications and has initiated steps to monitor confidentiality measures taken by telecom operators. More details are provided in the foregoing sections on Communications Surveillance and financial privacy respectively.

### 21.4.3 Consumer Protection Act 1986

The Consumer Protection Act which was enacted with the objective to provide for better protection of the interests of the consumer has emerged as a major source of relief to those who have suffered violations of their privacy. According to the Consumer Protection Act,1986, a consumer is a broad label for any person who buys any goods or services for consideration with the intent of using them for a non-commercial purpose. The Act creates a three tiered adjudicatory apparatus for the determination of consumer disputes, with the District Consumer Disputes Redressal Forum at the bottom, the State Consumer Disputes Redressal Commission occupying the intermediate tier and the National Consumer Disputes Redressal Commission at the apex. These Commissions have all the powers of a civil court to determine the issues before them. Complaints can be filed by consumers against traders or service providers for unfair trade practices[334] defective goods, deficiency in services, overcharging by a trader or service provider,

[334] Section 2(r) of the Consumer Protection Act 1986 contains a very elaborate definition of unfair trade practices running into nearly three pages and includes a number of trade practices "which, for the purpose of promoting the sale, use or supply of any goods or for the provision of any service, adopts any unfair method or unfair or deceptive practice including any of the following practices"

hazardous goods. Although the issue of violation of privacy has not arisen pointedly in too many consumer complaints, there are a few instances that stand out.

In *Rajinder Nagar Post Office vs. Sh Ashok Kriplani*[335] a post master was accused of not delivering a registered letter, opening it, and then returning it in a torn condition. It was determined that the tearing of the letter without delivery to addressee was a grave "deficiency in service" on the part of the appellant. It was ruled that the right of privacy of the respondent was infringed upon by the postman. Under the Consumer Protection Act 1986, compensation of Rs. 1000 was awarded as to the mental agony, harassment, and loss arising from the charge of deficiency in service.

The importance of this case lies in the willingness of the courts to treat breach of privacy as a "deficiency of service".

In January 2007, the Delhi State Consumer Disputes Redressal Commission imposed a fine of Rs. 75 lakh on a group of defendants including Airtel, ICICI and the American Express Bank for making unsolicited calls, messages and telemarketing.[336] The Commission held that these were 'unfair trade practices' under the Consumer Disputes Act, and also declared that every consumer annoyed by unsolicited telemarketing calls and text messages was to be compensated by a minimum of Rs 25,000.[337] Although this decision was overruled on appeal by the Delhi High Court in 2010, it confirms a trend of Consumer Dispute Redressal Commissions willing to take up cudgels on behalf of consumers for violations of their privacy.[338]

[335] Rajinder Nagar Post Office v. Sh Ashok Kriplani, (2009), http://goo.gl/1jQ6x (last visited Oct 10, 2011).

[336] Harish Nair, *Consumer court hangs up on telemarketers?*, HINDUSTAN TIMES, January 16, 2007, http://www.hindustantimes.com/Consumer-court-hangs-up-on-telemarketers-calls/Article1-200029.aspx (last visited Oct 10, 2011).

[337] Utkarsh Anand, *HC reverses order on telemarketing calls*, INDIAN EXPRESS, January 18, 2010, http://www.expressindia.com/latest-news/hc-reverses-order-on-telemarketing-calls/568442/ (last visited Oct 10, 2011).

[338] While agreeing with the Consumer Commission that cellular operators must ensure unsolicited commercial communications had to end, the High Court ruled that the Consumer Commission lacked the jurisdiction to pass such heavy penalties, or to decree a minimum compensation amount to future consumers. An appeal against the High Court decision is currently pending before the Supreme Court. *SC issues notices to Bharti, others over unsolicited calls*, BUSINESS STANDARD, August 26, 2010, http://business-standard.com/india/storypage.php?autono=106683&tp=on (last visited Oct 10, 2011).

## §22 Cultural Dynamics

- are there cultural considerations within the right to privacy that should be mentioned?

### 22.1 Gender

- are there gender privacy related issues to cover? e.g. sexual offence victims

### 22.2 Religion

- are there religion and privacy issues to consider?

### 22.3 Other

- are there any other privacy issues of national or local significance?