Laws relating to Data Protection in India

Mubashshir Sarshar, National Law University, Delhi

Available at: https://works.bepress.com/mubashshir/28/
LAWS RELATING TO DATA PROTECTION IN INDIA

National Law University, Delhi

---

1 Mubashhir Sarshar, Student at National Law University, Delhi
Table of Contents

List of Abbreviations i
List of Statutes ii
List of Cases iii

CHAPTER – I INTRODUCTION 1
CHAPTER – II THE EUROPEAN STANDARD 4
CHAPTER – III THE UNITED STATES POSITION 7
CHAPTER – IV CURRENT DATA PROTECTION LAWS IN INDIA 10
CHAPTER – V SHORTCOMINGS IN THE CURRENT INDIAN LAWS ON DATA 15
CHAPTER – VI EFFORTS TAKEN BY INDIA TOWARDS DATA PROTECTION 22
CHAPTER – VII THE FEASIBILITY OF THE GOVERNMENT’S UIDAI PROJECT FROM THE DATA PROTECTION ASPECT 25
CHAPTER – VIII A COMMENT ON THE MODEL RULES FORMULATED FOR DATA PROTECTION IN INDIA 30
CHAPTER – IX CONCLUSION 34

BIBLIOGRAPHY
List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>§.</td>
<td>Section</td>
</tr>
<tr>
<td>AIR</td>
<td>All India Report</td>
</tr>
<tr>
<td>Art.</td>
<td>Article</td>
</tr>
<tr>
<td>Ed.</td>
<td>edition</td>
</tr>
<tr>
<td>ILR</td>
<td>Indian Law Report</td>
</tr>
<tr>
<td>p.</td>
<td>page</td>
</tr>
<tr>
<td>Rev.</td>
<td>revised</td>
</tr>
<tr>
<td>s.</td>
<td>Section</td>
</tr>
<tr>
<td>U.S.</td>
<td>United States of America</td>
</tr>
<tr>
<td>UETA</td>
<td>United Electronic Transaction Act</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Vol.</td>
<td>Volume</td>
</tr>
<tr>
<td>Vol.</td>
<td>volume</td>
</tr>
<tr>
<td>WTO</td>
<td>World Trade Organization</td>
</tr>
</tbody>
</table>
List of Statutes

Constitution of India, 1949

Information Technology Act, No. 21 of 2000

Indian Copyright Act, 1957.

India Penal Code, 1860
List of Cases


Gujarat Water Supply and Sewage Board v. Unique Erectors (Guj) AIR 1989 SC 973

CHAPTER – I

INTRODUCTION

The protection of data finds its roots in the individual's right to privacy doctrine. The right to privacy has been explicitly contained in or has inferentially been found to exist in the constitutions of most developed nations and the jurisprudential parameters of privacy rights explored in various forums. However, the specific privacy issue related to protection of personal data became an issue of growing concern in progressive nations in the 1970s with the advent of computerized systems which could store and disseminate large amounts of information with relative ease via automated processes.

"Data protection refers to the set of privacy-motivated laws, policies and procedures that aim to minimize intrusion into respondents' privacy caused by the collection, storage and dissemination of personal data." It is the legal safeguard used to prevent misuse of information stored in computers - particularly information about individual people. Data protection encompasses control and management of the data creation and creation of basic rights and obligations and also stipulates penalties and remedies in case of misuse of the data.

In the United Kingdom, the Younger Committee on Privacy was instituted in the early 1970’s to make recommendations regarding the manipulation of computerized personal data. Similarly, in the United States, the Data Privacy Act of 1974 was enacted. Subsequent protection of the privacy of personal information was accomplished in the United Kingdom and the United States through various legislative enactments. However, the gold standard for data protection was established by the European Union in 1995 with the passage of E.U. Directive 95/46/EC. The Directive established comprehensive legislation for data protection, setting a high standard for non-E.U. Member States to meet. The European Union's regime impacted non-

---

4 Carey, supra note 1, at 1-3.
6 Ibid.
8 The Data Protection Act of 1984; Also see Carey, supra note 10, at 3.
E.U. member nations directly because under the Directive data could not be transferred to states which did not provide adequate standards for protection.

The term "data" has been defined under section 2(o) of the IT Act of 2000. Data is the "physical representation of information in a manner suitable for communication, interpretation, or processing by human beings or by automatic means." The definition of "data" and its protection in the Indian context, does not give a comprehensive understanding of the term.

1.1 Research scheme

The researcher, in the course of developing a model law for data protection in India based on the European directive and other related foreign legislations, would examine India’s recent baby steps taken in direction of data protection. These would include the proposed amendments to the IT Act, the formation of the Data Security Council of India under Nasscom, maintaining of the National Do-not-Call Register and the to-be introduced National Customer Preference Registry under TRAI. Also examined would be the challenges with respect to data protection in the upcoming cloud based computing networks in India with special emphasis on the viability in terms of security of data in the Indian government’s ambitious Unique Identification Authority of India (UIDAI) project.

Thus, after comparing and contrasting the already available data protection mechanisms in India, the researcher’s conclusion based on the hypothesis would be whether these existent laws relating to data protection are sufficient for the new age India or is there a need to develop a model law for data protection based on the European directive and other related foreign legislations soon.

1.2 Research Techniques for Data Collection

Research technique of analysis, critique, and review of the theories would be intended to be employed.

1.3 Research Methodology

The researcher has followed the doctrinal method of research throughout the project and the MLA system of formatting has been adopted by him.
1.4 Research Question and Hypothesis

The researcher in the course of this project has mainly aimed to research on the current data protection law in India and the shortcomings in the structure. Also he has undertaken to form a set of model rules on data protection in India. Hence the obvious research question which the researcher has framed in this context is whether the current structure of laws in India with respect to data protection in India is adequate with respect to the need.

The hypothesis for the above question is No.

1.5 Scheme of Chapterization

The first chapter would lay down a brief introduction to the topic. The second and third chapter would highlight the European standard and the United States position of data protection which generally forms the standard for the other countries to follow. Chapter four would then highlight the current data protection laws in India. Chapter five would lay down the shortcomings in the current Indian Laws on the topic. Chapter six would then illustrate the efforts taken by India towards Data protection. Chapter seven would then emphasize on the feasibility of the Government’s UIDAI Project from the Data Protection aspect. Chapter eight would then consist of a comment on the model rules formulated for data protection in India. Lastly, Chapter nine would conclude the project.

1.6 Footnoting Style to be adopted

National Law University standard style of footnoting will be followed throughout the project.
CHAPTER – II

THE EUROPEAN STANDARD

European Union Directive 95/46/EC (the "Directive") was adopted in October 1995 for the purpose of mandating standards within the then fifteen-member European community for the protection of personal data.\textsuperscript{10} As with all E.U. directives, the Directive was not self-implementing. It required all E.U. Member States to enact, no later than October 25, 1998, national legislation giving effect to its provisions to protect individual citizens' rights to privacy and to prevent the unauthorized dissemination of its citizens' personal information both within and outside the European Union.\textsuperscript{11}

The Directive proposes broad-brush, ‘umbrella' legislation encompassing all sectors of industry and all instances of collection and use of personal data. The Directive protects "the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data…”\textsuperscript{12} The processing of data can be wholly or partially by automatic means.\textsuperscript{13} Personal data encompasses information relating to an identified or identifiable natural person who "can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."\textsuperscript{14} ‘Processing of personal data' is defined as any operation performed upon personal data whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction…”\textsuperscript{15}

In essence, all personal data held must comply with the following principles:

\textsuperscript{10} Kevin Bloss, Raising or Razing the e-Curtain?: The EU Directive on the Protection of Personal Data, 9 Minn. J. Global Trade 645, 645 (2000)
\textsuperscript{12} Council Directive 95/46/EC, art. 1(1).
\textsuperscript{13} Ibid. Art. 3(1).
\textsuperscript{14} Ibid. Art. 2(a) (emphasis added).
\textsuperscript{15} Ibid. Art. 2(b).
i. Personal data must be "processed fairly and lawfully," with disclosure of the controller of the data, and disclosure of the purpose for which it is being collected;\(^\text{16}\)

ii. Personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;"\(^\text{17}\)

iii. Personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;"\(^\text{18}\)

iv. Personal data must be "accurate and, where necessary kept up to date." Reasonable steps must be taken to make certain that inaccurate, misleading or incomplete data is "erased or rectified;"\(^\text{19}\)

v. Personal data must be "kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which data were collected or for which they are further processed." Member States are required to establish "appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific" purposes.\(^\text{20}\)

With regard to enforcement of the data protection laws, the Directive requires E.U. Member States to provide judicial remedies to any individual whose rights to data privacy are violated.\(^\text{21}\) It also requires that Member States adopt suitable measures to ensure the implementation of the Directive, and to impose sanctions on the data collectors and processors for violations of any section of the Directive.\(^\text{22}\) Several E.U. Member States, including the United Kingdom and Italy, have adopted specialized courts with exclusive jurisdiction over intellectual property matters.\(^\text{23}\)

A critical aspect of the Directive is its impact on the global economy. Data transfer to third countries or regions outside the European Union is permitted only if the recipient nation provides an "adequate level of protection."\(^\text{24}\) Pursuant to this case-by-case approach under Article 25 of the Directive, the adequacy of the level of protection afforded by a third country is

---

\(^{16}\) Ibid. Art. 6.
\(^{18}\) Ibid.
\(^{19}\) Ibid.
\(^{20}\) Ibid.
\(^{22}\) Ibid, Art 24.
\(^{23}\) Infra notes 185-213 and accompanying text.
assessed by the European Commission, which produces a list of the countries that ensure an adequate level of protection by virtue of their domestic laws or international commitments for the protection of private lives, basic freedoms, and rights of individuals.\textsuperscript{25} Factors such as the nature of the data, the purpose and duration of the processing operation, the country of origin, the country of final destination, the rules of law in place in the third country, and the professional rules and security measures complied with in that country, are considered in reaching an "adequacy" determination.\textsuperscript{26} The fear of a prohibition on transferring data to a third country, with far reaching economic and trade repercussions has encouraged certain third countries to adopt data protection measures similar to those of the European Union.\textsuperscript{27} Adoption of such laws, it is hoped, will lead to a finding of adequacy by the European Commission, thereby preserving trade and economic relations of the third country with the European Union.\textsuperscript{28} At present, the European Commission has concluded that the laws of Switzerland, Isle of Man, Canada, Argentina, the United States, and Guernsey provide adequate protection.\textsuperscript{29}

The Directive mandates, and E.U. nations have adopted, a comprehensive legislative approach which requires creation of government data protection agencies, registration of databases with those agencies, and in some instances prior approval before personal data processing may begin. In contrast, the U.S. approach to data privacy is "sectoral" in that it relies on a mix of legislation, regulation, and self regulation. Starting with the Fair Credit Reporting Act - the first legislation in the United States to regulate private sector use and disclosure of personal information at a federal level - and later the Privacy Act of 1974, which was enacted due to concerns about breaches of privacy arising from computer databases, the United States has a system of data protection that is governed sector by sector.\textsuperscript{30} At a state level, numerous laws protect the privacy of individuals.\textsuperscript{31}

\textsuperscript{26} Council Directive 95/46/EC, Art. 25(2).
\textsuperscript{27} Ibid. at 388-89.
\textsuperscript{28} Ibid.
CHAPTER – III

THE UNITED STATES POSITION

The United States was concerned that its "sectoral" approach to data protection, quite different from the European Union's "umbrella' approach, would not meet the European Union's standards of "adequacy." Fearing a disruption of commerce between the United States and E.U. Member States that would hurt both businesses and consumers, the U.S. Department of Commerce entered into negotiations with the European Commission in 1997 in an attempt to resolve the looming trade disaster.32

In the year 2000 the U.S. Department of Commerce and the European Commission unveiled a "Safe Harbor" framework designed to bridge the differences between the E.U. and U.S. approaches to privacy protection.33 On July 27, 2000, the European Commission determined that the U.S. Safe Harbor privacy principles provided adequate protection under Article 25(6) of the Directive.34 The finding of adequacy is binding on the Member States of the European Union, and permits U.S. organizations which participate in Safe Harbor to be deemed adequate under the Directive. By eliminating the need for approval from the European Union prior to data transfers, the process of transferring data to U.S. Safe Harbor entities is streamlined, and the continued flow of data to these U.S. companies is assured.35 Organizations formed in the United States are eligible to participate in the Safe Harbor agreement.36

Safe Harbor is essentially a self-regulatory approach whereby U.S. entities self-certify that they are complying with the principles of Safe Harbor.37 The Safe Harbor principles track the principles contained in the Directive, closing any loops that may exist between the U.S. sectoral laws and the requirements of the Directive. The seven Safe Harbor Principles are

33 Ibid.
i. Conspicuous notice must be provided to the data subject regarding the purpose of the data collection and use, as well as regarding complaint mechanisms available to the data subject.

ii. Choice must be offered to the data subject to opt out if the data is being used for a purpose that is different than its original purpose, or if data is to be transferred to third parties. The data subject is given an opt-in choice if the data is sensitive, relating to race, religion, ethnicity etc.

iii. Onward transfer of personal data to third parties may only be done consistent with the principles of notice and choice.

iv. The data subject must be permitted access to his or her information collected by the U.S. entity.

v. The security of the personal data must be maintained by exercising reasonable precaution to ensure that data is protected from loss.

vi. The integrity of data must be maintained, ensuring that it is relevant to the purpose for which it was collected, accurate and current.

vii. The self-certifying U.S. entity must provide mechanisms for enforcement of the Safe Harbor principles. Data subjects must be provided a forum for filing complaints, and a dispute resolution procedure established to respond to grievances of the consumer.\(^{38}\)

Organizations in the United States may incorporate the seven Safe Harbor principles in various ways. For instance, organizations may adopt safeguards deemed necessary by the European Union for transfers of personal data from the E.U. to the U.S. by incorporating the relevant safe harbor principles into agreements entered into with parties transferring personal data from the European Union.\(^{39}\) In the alternative, where an organization is subject to U.S. statutory, regulatory, administrative or another body of law (or bodies of rules issued by national securities exchanges, registered securities associations, etc.) that also effectively protects personal data privacy, it qualifies for Safe Harbor to the extent that there is a nexus between its activities and the specific laws or rules.\(^{40}\) With regard to enforcement of data privacy laws, given the U.S.’s sectoral approach, violations of data privacy in the United States may be prosecuted by


\(^{39}\) Supra Note 28.

federal or state authorities in corresponding courts, or by the administrative agency under whose jurisdiction the sector is being regulated or legislated.\textsuperscript{41} Although the United States has adopted a number of specialized courts, at present none deal exclusively with data privacy matters.

Breaches in data security, such as that reported by Lexis-Nexis in March 2005 involving personal information of 32,000 U.S. residents\textsuperscript{42}, as well as by the shoe retailer DSW Inc., which reported that credit card numbers of people who shopped at 103 of its 175 stores had been obtained by hackers, have not helped to build confidence in the U.S.’s data protection regime. U.S. companies reported more than sixty data breaches between January and September 2005, and Congress, as well as a number of state legislatures, responded with dozens of pieces of legislation, many modeled after a 2003 California law requiring companies to notify affected customers about data breaches.\textsuperscript{43} In November 2005 the Senate Judiciary Committee was referred a bill that would require companies with data breaches to notify affected customers, and would set up rules for the U.S. government’s use of private databases.\textsuperscript{44} The bill would require businesses holding the personal data of more than 10,000 U.S. residents to conduct risk assessments and implement data-protection policies.\textsuperscript{45} Failure to implement security plans could expose businesses to fines of up to $35,000 per day.\textsuperscript{46} Despite the outcry over the dozens of breaches this year, Congress has been reluctant to pass a data breach notification bill, partly because of growing concerns that most of the bills would take a step backward from existing state laws.\textsuperscript{47}

\begin{itemize}
\item \textsuperscript{43} Identity Theft Protection Act was introduced in July 2005. S. 1408, 109th Cong. (2005).
\item \textsuperscript{44} Personal Data Privacy and Security Act of 2005, S. 1789, 109th Cong. (2005).
\item \textsuperscript{45} Ibid.
\item \textsuperscript{46} Ibid.
\end{itemize}
CHAPTER – IV

CURRENT DATA PROTECTION LAWS IN INDIA

In India, the protection of privacy, a basic human right recognized by the Universal Declaration of Human Rights of 1948, was derived from common law torts and constitutional law. A person may be held tortiously liable for unlawful invasion of privacy of another, whereas under constitutional law, this right has been implicitly recognized, but is subject to reasonable State-imposed restrictions. However, the IT Act of 2000 is considered to be the most widely recognized legislation that covers data protection. In order to cover the shortcoming in the IT Act of 2000, contractual clauses that the Indian companies have agreed to come into play in the trade with overseas clients.

4.1 Constitutional Law

The protection of data finds its roots in the individual's right to privacy. In a number of decisions, the Supreme Court of India has upheld the right to privacy as a fundamental right. Moreover, Article 300A of the Constitution of India, provides for the right to property as a constitutional right. This makes intellectual property in the data a subject of this right.

To adhere to the international human rights instruments (International Covenant on Civil and Political Rights, International Covenant on Economic Social Cultural Rights, and

51 Constitution of India, Art. 21.
52 NASSCOM Announces Milestones for Its 'Trusted Sourcing' Initiative, NASSCOM
53 Vakul Sharma, Legal Issues for Data Protection: Myths and Realities.
54 Supra note 1.
57 Constitution of India, Art. 300A.
Universal Declaration of Human Rights\textsuperscript{61}, the Indian Parliament has enacted a variety of legislation to safeguard recognized human rights. For example, the Protection for Human Rights Act of 1993 provides for the constitution of a National and State Human Rights Commission and Human Rights Courts for better protection of Human Rights and for connected or incidental matters.\textsuperscript{62}

### 4.2 Information Technology Act of 2000

The IT Act of 2000 is considered to be the law that governs data and its protection.\textsuperscript{63} When the IT Act of 2000 was passed, the concept of "data protection" was not envisaged. The only safeguard that the IT Act of 2000 provides to data is with respect to the penalty in a case of breach or unlawful activity. The provision under the IT Act of 2000 that deals with unauthorized access and damage to data is Section 43.\textsuperscript{64} Section 43(b) affords cursory safeguards against breaches in data protection. The scope of Section 43(b) is limited to the unauthorized access, downloading, copying, extraction, or damage of data from a computer system.\textsuperscript{65} However, the Information Technology (Amendment) Act of 2008\textsuperscript{66} has removed any cap on the amount of damages.\textsuperscript{67} The damages under Section 43 were quantified at Rupees one crore, but the IT Act of 2008 has removed this limit of one crore and made the damages unliquidated; thus, the damages that one can suffer under these instances can be well above Rupees one crore.\textsuperscript{68}

Section 43-A of the IT Act of 2008 deals with compensation for failure to protect data by a corporation involved in "possessing, dealing, or handling any sensitive personal data or information in a computer resource which it owns, controls, or operates" and "causes wrongful loss or wrongful gain to any person."\textsuperscript{69} In order to ensure that a corporation is liable under this section, it has to be proved that the corporation was negligent in implementing "reasonable security practices and procedures."\textsuperscript{70} This section places liability on an intermediary as well.\textsuperscript{71}

\begin{itemize}
\item \textsuperscript{62} Protection for Human Rights Act, No. 10 of 1993.
\item \textsuperscript{63} Information Technology Act, No. 21 of 2000
\item \textsuperscript{64} Information Technology Act, No. 21 of 2000, Section 43.
\item \textsuperscript{65} Ibid.
\item \textsuperscript{66} Information Technology Act, No. 21 of 2000, Section 43A.
\item \textsuperscript{67} Ibid.
\item \textsuperscript{68} Ibid.
\item \textsuperscript{69} Ibid.
\item \textsuperscript{70} Ibid.
\item \textsuperscript{71} Ibid.
\end{itemize}
However, the liability of an intermediary sued under section 43-A is diluted in section 79 of the Act, which inserts both "knowledge" and "best efforts" as qualifiers prior to assessing penalties. Moreover, section 85 of the IT Act of 2008 also invokes entity liability, limited to the specified illegal acts of persons for intentional or negligent acts that result in a breach of the specific violations under the IT Act of 2000.

4.3 Intellectual Property Rights Laws

Computer software (including computer programs, databases, computer files, preparatory design material, and associated printed documentation, such as users' manuals) receives copyright protection under Indian laws. The Indian Copyright Act of 1957 "prescribes mandatory punishment for piracy of copyrighted matter commensurate with the gravity of the offense." Computer programs are not per se patentable, being patentable only in combination with hardware. Thus in India, by past practice and under current laws, copyright is the preferred mode of protection for computer software.

4.4 Criminal Laws

Under the Indian Penal Code of 1860 ("IPC"), there is no express criminal punishment for breaching data privacy, thus "liability for data-related breaches must be inferred from tangentially related crimes." For example, "Section 403 of the Indian Penal Code imposes criminal penalty for dishonest misappropriation or conversion of 'movable property' for one's own use." Therefore, "although no jurisprudence has been developed on this interpretation, arguably, movable property encompasses computer-related data and intellectual property." There is an element of trust involved when a person discloses his or her personal information to

71 Ibid.
72 Information Technology Act, No. 21 of 2000, Section 79.
73 Section 63B of the Indian Copyright Act of 1957.
74 Section 2(o) of the Indian Copyright Act of 1957.
78 India Penal Code, Section 403.
79 Supra note 76.
another. In the case where this information is disclosed to a third party, it could result in criminal penalties for the criminal breach of trust.\textsuperscript{80} Further, the IPC imposes criminal liability for dishonest or fraudulent concealment or removal of property\textsuperscript{81}, and also for when a person "cheats and thereby dishonestly induces the person" in possession of the property to deliver the said property.\textsuperscript{82} Furthermore, section 425 imposes liability on a third party who intends to cause wrongful loss or damage to the property of another person, whether or not the person is the owner of the property.\textsuperscript{83}

### 4.5 Contractual Obligations

Non-E.U. states where data protection has not been found to be "adequate,"\textsuperscript{84} such as in India\textsuperscript{85}, rely on an alternative avenue and ad hoc solutions to procure and continue business transactions. The European Commission and the Data Protection Commissioner have the power to endorse "model contracts" specific to the transferring countries' circumstances, as well as the power to approve particular contracts or other arrangements that provide satisfactory safeguards.\textsuperscript{86} Data Exporters in other countries enter into a contract with an Indian BPO detailing the specific duties and obligations of both parties involved. Therefore, in the absence of legislation that offers sufficient and adequate legal protection for personal data, any uncertainty regarding doing business with an Indian BPO is a matter of negotiation of the relevant contract using appropriate legal expertise and advice. Apart from contractual obligations with the Data Exporters, the employment contracts between the BPO and its employees also specify that the employees have to maintain confidentiality regarding all such information that they may process.\textsuperscript{87}

---

\textsuperscript{80} Indian Penal Code, Section 405.  
\textsuperscript{81} Indian Penal Code, Section 424.  
\textsuperscript{82} Indian Penal Code, Section 420.  
\textsuperscript{83} Indian Penal Code, Section 425.  
\textsuperscript{85} Ibid.  
\textsuperscript{87} Ibid.
4.6 The Credit Information Companies (Regulation) Act of 2005

The Credit Information Companies (Regulation) Act of 2005 "imposes duties on credit information companies, credit institutions, and specified users while processing credit data." Additionally, the Reserve Bank of India has the authority to penalize any credit information company, credit institution, or specified user, for violating this Act. On this ground, the "Reserve Bank of India could be considered as a specific data protection authority in the field of credit information."

---

89 Ibid.
90 Ibid.
CHAPTER – V
SHORTCOMINGS IN THE CURRENT INDIAN LAWS ON DATA PROTECTION

Although India has been proactive in making provisions for the protection of data, it has a long way to go in order to reach the heights of protection afforded by international provisions for data protection in foreign countries. The protection of data in India needs to be critically examined and the lacuna must be spotted. Only then can a measure for its elimination be taken. The shortcomings in the national data protection laws may be examined as follows

5.1 Information Technology Act of 2000

The major shortcoming in the IT Act of 2000, as amended by the IT Act of 2008, is that none of the three objectives detailed in the preamble\(^{91}\) recognize the protection and preservation of data. The very fact that data protection is outside the scope and purpose of the IT Act weakens the relevance of its provisions. Moreover, "data" under the IT Act of 2000 is restricted to data stored and processed in the electronic form.\(^{92}\) Considering that India still employs conventional methods of data storage, transfer, and process, all forms of data other than electronic data are susceptible to unauthorized use that might adversely affect the subjects of such data. Therefore, this legislation does not provide protection to data stored in the non-electronic medium.

Section 43 penalizes any unauthorized access to a computer, computer system or computer network and any unauthorized download, copying or extraction of any data.\(^{93}\) An interpretation of section 43 shows that it provides for protection of data in a very limited sense - it is only a punitive provision.\(^{94}\) The IT Act of 2000 penalizes any individual who misuses electronic data, without the permission of the owner or any other person in charge of such data. This penalty is inadequate because it does not address the concern of misuse of data by the person responsible for such data. Section 43 does not address data protection. Rather, it is merely

\(^{91}\) Information Technology Act, No. 21 of 2000,
\(^{92}\) Information Technology Act, No. 21 of 2000, S. 2(o).
\(^{93}\) Information Technology Act, No. 21 of 2000, S.43.
\(^{94}\) Ibid.
recourse to compensate the individual for any damage resulting from unauthorized access or damage to data.

"Data protection" in its entirety means the collection, retention, protection and proper disposal of the data collected.\(^95\) Therefore, section 43 of the IT Act of 2000 is very limited because it only provides a remedy for unauthorized access or damage to stored data. It does not address many of the principles provided in the Data Protection Act of 1998 (DPA).

In the provisions under the DPA in the U.K., personal information and sensitive personal information have different levels of protection, where loss, unauthorized access or disclosure of sensitive personal information is considered to have a deeper impact on the data subject.\(^96\) In contrast to the DPA, the IT Act of 2000 does not assign a higher level of care or protection to sensitive personal information. In essence, there is no difference between personal information and sensitive personal information in relation to data protection. Indeed, "personal information" is not defined in judicial precedent or the IT Act of 2008. Because this term has not been defined, it is difficult to give an exact interpretation of the provisions.

Section 43-A of the IT Act of 2008 places liability on a corporate body only if it has been negligent in implementing its security practices and procedures in relation to the data possessed, controlled or handled by it.\(^97\) There is a significant difference between "negligence to implement" and "failure to implement." The former requires the test of reasonableness to be satisfied before there can be any claim of negligence, while the latter requires only non-performance of the required action. Therefore, there is no liability for the corporate body in cases of failure to implement its security practices and procedures, thereby widening their scope for escaping liability.

The terms "wrongful gain" and "wrongful loss" are used under section 43-A of the IT Act of 2008.\(^98\) However, these terms have not been clearly defined with relevance to data protection, either under statutes or any judicial precedents. It is unclear whether these terms derive their meaning from their definition under the substantive penal law of India, the Indian Penal Code of

\(^{95}\) Ibid.
\(^{96}\) Data Protection Act, 1998 (Eng.)
\(^{97}\) Information Technology (Amendment) Act, 2008, Section 43-A.
\(^{98}\) Ibid.
1860. Therefore, it is difficult to comprehend the true meaning and application of this section in light of these undefined terms.

The section also makes a reference to "reasonable security practices and procedures," which has been defined under the IT Act of 2008. The three methods by which reasonable security practices and procedures can be determined are: 1) by agreement; 2) by law; and 3) by prescription by the Central Government. However, there is no law in India that defines this term and it will be some time before the Central Government promulgates the necessary regulations to give meaning to this term. Until these regulations are created, a corporation is not liable if the corporation does not agree with the person providing the information to define reasonable security practices and procedures, and then proceeds to disclose that information, even if the corporation causes loss or gain to that person. Thus, the protections are meaningless.

Under the IT Act of 2008, section 43-A places liability on an intermediary as well. However, an intermediary sued under section 43-A, can claim immunity under section 79, if the intermediary satisfies the test laid down under section 79. Therefore, although the law creates personal liability for illegal or unauthorized acts, little effort is made to ensure that Internet service providers or network service providers, as well as entities handling data, are responsible for the safe distribution or processing of the data.

Section 72-A clearly requires that a person who discloses personal information, thereby causing wrongful loss or gain, to have done so willfully. Hence, in order to make a person liable it has to be proved that the person disclosing the personal information did so with an intention to cause wrongful loss or gain. Mere proof of the damage is insufficient. Moreover, section 72-A does not help individuals monetarily. It imposes penal consequences on such persons by way of a fine, which is insufficient to compensate the injured party.

99 Ibid.
100 Ibid.
101 Information Technology (Amendment) Act, 2008, Section 79.
102 Supra note 76.
103 Supra note. 100.
104 Ibid.
105 Ibid.
106 Ibid.
Further, section 72-A is restricted to information about individuals and relates only to personal information obtained under service contracts.107 This section also makes it evident that disclosure of personal information with intent to cause wrongful loss or gain has to be done without the consent of the person, whose personal information is being disclosed.108 It may be stated that this provision has not been drafted to cover all situations. In many cases, corporations and individuals when entering into service contracts, ensure that they obtain consent of the individuals for any future disclosures. There are also standard form contracts where the clauses cannot be negotiated - the parties must accept all clauses. Hence, if disclosure of information is one of the clauses in such contracts, then any disclosure is deemed to be with the consent of the person concerned. Therefore, if such a corporation obtains the individual's consent at the time of entering into service contracts, the protection provided for under this section does not apply. The "consent" referred to in section 72-A can be easily circumvented by corporations and individuals by means of clever drafting when entering into service contracts.

Section 72 is insufficient because the section only applies if the breach is committed by a person who has been conferred certain powers under the Act, rules, or regulations.109

The Indian laws do not specify conditions under which data can be collected and used, and its limited scope fails to meet the breadth and depth of protection that the E.U. Directive mandates.110 The Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data, 1980 promulgated by the OECD are also instructive, demonstrating that a large void exists in India's IT Act of 2000.111

5.2 Criminal Laws

The protection provided by criminal laws is not sufficient in the context of data protection. At the time of enactment of the IPC, it was not envisioned that the provisions would be used to provide data protection. Although the IT Act of 2000 and IT Act of 2008 have made amendments to the IPC, there has been no change with regard to the application of the IPC to data protection. The meaning of "movable property" is unclear as to whether it extends to include

---

107 Ibid.
108 Ibid.
109 Ibid.
110 Supra note 76.
111 Ibid.
intellectual property. Moreover, the adequacy of the remedies under India's criminal laws is questionable in a trans-national context. As correctly pointed out, "the cost, delay and inconvenience associated with foreign nationals bringing actions in Indian courts offsets the availability of the recourse."

5.3 Intellectual Property Rights Laws

On perusal of the Indian Copyright Act of 1956, it is evident that the Act does not afford complete protection to data. The penalties under this Act are inadequate in a trans-national context. Moreover, the backlog of cases in the Indian criminal courts is not only detrimental to the enforcement of copyright laws on the national and international front, but it also prolongs litigation. Further, there would be the question of conflicting rights and jurisdictions, thereby duplicating litigation.

5.4 Contractual Obligations

It is pertinent to note that although the gap in the laws is sought to be filled through contractual recourse, it may not be very effective in the absence of strict laws backing it up. The major drawback in use of model contracts is that the Indian BPO is subject to the jurisdiction of an E.U. Member State and the data protection authority, and any departure from the standard clauses runs the risk of disapproval of the contract by the data protection authority.

In contracts for the transfer of data, a number of third parties may be involved: first, the data subjects; second, the third parties to whom the data is to be re-exported by the importer; and last, the data protection authorities. However, in the case of breach of contract, the injured party may only seek a remedy against the contracting party. The injured third party may not have proper recourse against the actual wrong-doer. Moreover, in relations with third parties, dispute resolution clauses in the contract between the BPO and the Data Exporter are likely to be of very limited effect. The determination as to the governing law or the competent adjudicating authority will, therefore, be difficult to impose on the third parties in the event of a dispute.

---

113 Section 62 of the Indian Copyright Act of 1957.
Moreover, the clause indemnifying any loss caused by a third party could prove to be detrimental to the party indemnifying the loss. The third party causing the loss could escape liability and the party to the contract, dealing with that third party, would be responsible instead. Another shortcoming in the application of contractual laws for protection of data is that some outsourcing agreements include a clause limiting the liability of the party. It contains a cap on the amount or extent of damages for which a party may be liable.\textsuperscript{115} While this clause, detailing the liquidated damages, makes assessment of the same easier and excludes interference by the courts, it also requires an accurate pre-estimate of the possible damage, which, if not properly calculated, could result in loss to the injured party.

\textbf{5.5 Researcher’s suggestions towards a reform in the protection codes}

The Indian system of data protection can be best described as a web, i.e. many protections are offered through various sources and the web traps some violations, but gaps and holes remain through which others slide through. In order to address the inadequacies of the IT Act of 2000 and the miscellaneous laws providing protection of data, Indian businesses and the Indian government drafted amendments which would fill the voids. Although passage of the amended law covering data protection was anticipated in 2004, the proposed legislation was shelved due to a change in government in 2004.\textsuperscript{116} Whether the IT Act is amended, or alternative legislation enacted to protect the sanctity of transferred data, the new laws must offer effective enforcement in order to conform to the "adequacy" norms of the Directive and the Safe Harbor privacy principles of the U.S. After the new rules are in force, India will enter discussions with the E.U. to get recognition as a country that offers an adequate level of protection for personal data.

Enactment of law that facially provides protection is but one step in the fight to maintain the sanctity of data. Even if satisfactory data protection laws are in place in India, the real question in assessing the adequacy of the law is whether these laws will be effective in deterring wrongful data piracy. Two issues are examined in this context. The first general issue is whether punishment deters crime. If it is concluded that appropriate sanctions do prevent and deter crime, the second issue is whether wrongful appropriation of data will be prosecuted in India.

\textsuperscript{115} Bharath Vagadia, Outsourcing to India: A Legal Handbook 57 (Verlag Berlin Heidelberg: Springer, 2007).
\textsuperscript{116} An amendment to the IT Act of 2000.
sufficiently so as to be a deterrent. If the Indian enforcement system is found inadequate, alternative enforcement processes must be established to prosecute violations of data privacy. A system of specialized courts instituted in India to prosecute cyber infringement cases, including data privacy violations, is essential for this purpose.

Once the data protection laws in India are strengthened, the general legal system must be tweaked in order to address data protection enforcement. Proposed remedies to fix the enforcement void include establishment of a national centralized enforcement body dedicated to, and trained in, electronic data piracy and enforcement. This national body must be given jurisdictional authority to enforce across state borders. In addition, it is essential to have specialized local police enforcement units which are specifically trained and maintained to recognize instances of, and enforce actions against, data piracy crimes. Finally, it is vital to adopt meaningful court reform to decrease burdens, costs and delays, and ensure that cases are concluded promptly with deterrent penalties and damages.
CHAPTER – VI

EFFORTS TAKEN BY INDIA TOWARDS DATA PROTECTION

Instances of data theft have compelled both the government and the industry to remedy the situation as a response to international pressure, in terms of providing some sort of framework for data protection. The researcher has narrowed down to two major of these efforts and discussed them in this chapter.

6.1 Setting up of the Data Security Council of India

The National Association of Software and Services Companies (NASSCOM) has set up a self-regulatory initiative in data security and privacy protection called the Data Security Council of India (DSCI). What led to the establishment of the DSCI is the continuing effort by NASSCOM to ensure that the Indian information technology industry has a safe environment that can be benchmarked with the rest of the world.

The DSCI is a self-regulatory body established under the premise that the industry, rather than the government, is best positioned to develop appropriate data privacy and security standards as it has greater knowledge and better understanding of the practical commercial issues involved. It is felt that such an approach would allow the DSCI to evolve and effectively respond to global developments. The DSCI would adopt global standards in order to move towards this end, initially focussing on establishing its membership and evolving a code of conduct by promoting a culture of privacy. Initially, the DSCI would promote and encourage voluntary compliance with the code of conduct, gradually creating a mechanism for enforcement of the same in an effort to establish its credibility.\(^{117}\)

The DSCI is envisaged as a non-profit organisation, with its governing body having an adequate representation of independent directors and industry specialists. Organisations associated with data security and privacy protection such as Information Technology (IT) and Information Technology enabled Services (ITeS) companies, academic or research institutions and universities can also become members of the DSC.

Its stated mission can be summarized in a form of five distinct points. They are-

i. Enable IT and ITeS companies to provide a high standard of security and data protection by adopting best practices.

ii. Develop monitor and enforce an appropriate security and data protection standard for the Indian IT and ITeS industry that would be adequate, cost effective, adaptable and comparable with global standards.

iii. Build capacity to provide security certification for organizations

iv. Create a common platform to promote the sharing of knowledge about information security and foster a community of security professionals and firms.

v. Create awareness among industry professionals and other stakeholders about security and privacy issues.

6.2 National Do Not Call Register

As discussed at the very outset, any data protection law should aim at protecting the privacy of data and, at the same time, ensuring the free movement of data. The issue of privacy of personal data, especially personal telephone numbers, has been the subject of great discussion among legal and industry circles in the recent past in India. The multiplicity of telecommunication service providers, coupled with easy and inexpensive mobile phone connectivity has led to rampant breaches of the personal privacy of mobile phone users. Taking advantage of the enormous amounts of freely available mobile phone user data, many industries in the finance, banking, health and tourism sectors have set up telemarketing services to tap the potential business opportunities that lie in such data. Consequently, telemarketing calls have become yet another intrusion introduced by the digital revolution in the lives of Indians, and what initially appeared to be a matter of routine inquiries regarding loans or credit card requirements turned out to be a massive and unabated nuisance to the receivers of such calls.

Eventually, the Telecom Regulatory Authority of India (TRAI) had to take steps to curb these unsolicited commercial calls pursuant to a petition filed by a Delhi-based lawyer before the Delhi State Consumer Dispute Redressal Commission against a leading private telecom company, Airtel, along with two banks, on various counts including breach of privacy, financial loss, mental harassment and agony, and wrongful gain by the respondents. While allowing the petition and passing severe strictures against the respondents, the Commission also directed the establishment of a National 'Do Not Call' Register by TRAI, which would bind all the players in
the market, placing special emphasis on the fact that commercial telemarketers could not call a subscriber if their number was on this Register. On the establishment of such Register, subscribers would be called upon to register their telephone numbers free of cost through the Internet by publicising such a Register in the newspapers.

6.3 Researchers critical Analysis of these Steps taken towards Data Protection

While the efforts made by NASSCOM in establishing the DSCI are commendable, only time would tell whether the self-regulation of an industry of this sort is a lotus-eater's vision or an achievable dream. The DSCI's stated mission is extremely encouraging in these times, when data security is one of the major concerns for foreign investors in India. The DSCI would have to build up a sufficient membership, with the willingness to comply with its code of conduct, before it can push forward its stated objectives. If and when a data protection law is enacted by India, the DSCI could play a pivotal role in administering such a law. While it is too early to comment on how effective the DSCI is in data protection, it certainly is a positive step in that direction.

The effect of the establishment of the National 'Do Not Call' Register on telemarketing calls has been quite dramatic, in that there has been a remarkable slide in the number of calls to those who took the effort to opt out by registering in the register under the NDNC. Also, as in the case of the DSCI, it is too early in the day to comment on the NDNC's functioning or its efforts to protect data privacy.
CHAPTER – VII
THE FEASIBILITY OF THE GOVERNMENT’S UIDAI PROJECT FROM THE DATA PROTECTION ASPECT

The Unique Identification Authority of India (UIDAI) was established in February 2009, for the purpose\(^{118}\) of issuing a unique identification number (UID) to all Indian residents that (a) is robust enough to eliminate duplicate and fake identities, and (b) can be verified and authenticated in an easy, cost effective way.

A key necessity of the UID system is to reduce/eliminate duplicate identity in order to improve the efficiency of the service delivery of various government initiatives. UIDAI has chosen biometrics feature set as the primary method to check for duplicate identity. In order to ensure that an individual is uniquely identified, it is necessary to ensure that the captured biometric information is capable of enabling de-duplication, accurately, at the time of collection of a person’s information resident in India.

As UIDAI proposes to use common demographic data for establishing and verifying identity, it becomes critical to standardize these fields and the verification procedure across registrars and to aid interoperability across many systems that will be used to capture, and work with resident identity.

Security and Privacy Challenges in UIDAI Project

The basic requirement and objective of UIDAI is to uniquely identify an individual out of a population of 1.2 billion people and to eliminate duplicate identity. UIDAI has selected biometrics feature set as the primary method to check for duplicate identity. Taking into consideration the data protection regime which India expects to create for itself, the researcher would go on to discuss the security and privacy issues related in the UIDAI project.

Before we understand the security issues surrounding biometrics we need to understand the fundamentals of identity and authentication.\(^{119}\) “An identity is defined as “who you are”, while dealing with authentication, it is defined as “How can you prove it”. A system must maintain distinct mechanisms for identity and authentication. Identity must be unique; Authenticators, however, don’t have to be unique only secret. Now consider biometrics - Given

\(^{118}\) [http://uidai.gov.in/documents/Creating a unique identity for every resident in India.pdf](http://uidai.gov.in/documents/Creating a unique identity for every resident in India.pdf)

the definitions and characteristics of identity and authentication, what is biometrics: identity or authentication?

Let’s think about the attributes of biometrics. Is it public or private? Public, of course. We leave various biometrics everywhere we go -- our fingerprints remain on anything we touch, our face is stored in countless surveillance systems, our retina patterns are known at least by optometrist, perhaps. And it’s believed, although there is no actual evidence to support the claim, that biometrics are unique. It follows that biometrics are identity, not authentication.

Identity and authentication are distinct components of the steps necessary to use a secure system. Identity without authentication lacks proof; authentication without identity invalidates auditing and eliminates multi-user capability.

Consider the UIDAI system where biometrics is the only system used for uniquely identifying an individual. In such a system biometric is now serving both; to identify you and to prove that you are you. In a system, where authentication is based on a simple password there is a possibility of changing a password, if a bad guy learns your password; but what if he gets your biometric spoofed how you will change it, something you have is unique to you. Further, it should be evident that the loss or theft of one’s biometric image opens the door to massive identity theft if the thief can use the biometric for his or her own purposes. But, because people usually only have two thumbs, two eyes, and one head, it is nearly impossible to change these, if and when the related biometric data become compromised. In this sense biometrics operate like shared secrets or passwords – learn the secret and you’re in. But there are some very important differences between biometrics and passwords: you cannot change them and have no choice but to keep them for life. Hence, it is better to have additional parameters which are private and belong to the category of “something you know”.

Further, there has been no proven technology for Biometrics which is 100% accurate. The best system was accurate 98.6 percent of the time on single-finger tests, 99.6 percent of the time on two-finger tests, and 99.9 percent of the time for tests involving four or more fingers. These accuracies were obtained for a false positive rate of 0.01 percent. (National Institute of Standards and Technology (NIST) tested 34 commercially available systems provided by 18 companies from around the world) So even considering a situation wherein there is 99.99% accuracy in the biometric, we can see that out of 1.2 billion people, 120,000 people will have false positives.
Further, considering the technology and amount of information that will be stored in the form of biometrics; it is estimated that the amount of data will approximately be equivalent to 10,215 TB as per Biometric committee report.

**Critical Analysis of the UIDAI Project**

The UID authority will only issue a unique identifier - a randomized number – that will only identify a person with his attributes that will include biometric information (Fingerprints, IRIS, Face). It is clear that only the biometric information will be unique to an individual, and will be used for de-duplication process. While name, photograph, address etc of a person may not be entirely private, since these can be obtained from various sources, it is the biometric information which is unique to an individual that is claimed to be highly confidential and personal, even though we have pointed to evidence contrary to this. This attribute is not only personal to an individual, but it is permanent and does not change significantly over a lifetime for an adult. Compromise of biometrics of a person will have serious consequences for an individual throughout his life.

The researcher would point out the security vulnerabilities of a biometric system, and possibilities of data compromise that can lead to the loss of privacy of an individual due to-

i. Spoofing  
ii. Replay attacks  
iii. Substitution attack  
iv. Tampering  
v. Masquerade attack  
vi. Trojan horse attacks  
vii. Overriding Yes/No response  

According to the proposal, UIDAI will store the information in CIDR – Central ID Registry to be operated by the Authority. One can trust that the Authority will create CIDR with the best of physical security and other appropriate technologies and processes to secure the data and prevent unauthorized access, with the caveats noted above. However, the documents that have been made public reveal that the registrars and sub-registrars and also enrolment agencies which might number in millions throughout the country, will also store such data on a local
basis. The registrars will be required to maintain this data of the people that they have identified and enrolled, since they will be required to update records whenever some of the fields change – in particular for the children, biometrics will have to be updated every 5 years, while for adults biometrics may have to be updated every 10 years. The registrars, subregistrars and other enrolment agencies therefore become the weakest link where adequate security measures for protection of data may be lacking. Given the cases that have been in the limelight recently such as the infamous rape, molestation cases where the Law Enforcement agencies, bureaucracy and the politicians have abused the system; as also India being one of the more corrupt countries, abuse of all these local repositories throughout the country by powerful persons is a strong possibility.

The researcher has made the observed that Biometric Encryption technology affords a solution that is fully secure, and at the same time protects privacy of individuals since it is based on biometrics being used to encrypt a PIN that is unique to a person – it does not require biometrics to be stored.

The Demographic Data Standards and Verification Procedure Committee Report submitted on December 9, 2009 has identified the key demographic data of residents that need to be captured along with the unique identifier, under the Know Your Resident (KYR) program for which KYR process and supporting documentation have been detailed. While the supporting documentation includes Proof of Identity (POI), Proof of Address (POA) and Proof of Date of Birth (POD) documents, these are based on generally acceptable documents such as Passport, PAN, Ration Card, Gas connection, Driver license etc.

However, for the millions of rural residents, migrant workers and others, who have no POI or POA documents, and UID is supposed to benefit them the most, as well as help plug-in the loopholes for saving of government funds in socially important schemes such as National Rural Employment Guarantee (NREG) Scheme, an Introducer System has been proposed. This system is on the lines of opening of a bank account, where someone already having an account introduces another person to open a bank account. In this case, any person who has obtained a UID can introduce others for issuance of a UID. Clearly, those who are in the greatest need of UID are once again left to the mercy of “Privilege Persons” – those having UIDs such as the BDOs, Sarpanches, NGOs and other “Gram Sevaks”.

If these functionaries in a rural area wish, only then a dispossessed, landless labourer or a similar person will be able to obtain a UID. This will take over 60% of the population back to square one, and they will have to resort to bribery and fulfill other demands of the “Privilege Persons” to obtain UIDs.
CHAPTER – VIII
A COMMENT ON THE MODEL RULES FORMULATED FOR DATA PROTECTION IN INDIA

On February 7, 2011, the Department of Information Technology, MCIT published a draft of a set of rules to be known as the ‘The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011’ in exercise of the powers conferred by Section 87(2)(ob), read with Section 43A of the Information Technology Act, 2000 to it. The set of rules came into force on April 11 this year upon its publication in the official gazette of India.

The researcher in this respect has tried to understand this most recent government initiative towards a strong data protection regime in India and has thus tried to suggest some further improvements in these set of rules in order for them to come to the standards of the protection offered under the European Union and the UK Data Protection laws.

They rules are as follows-

i. **Rule 3** - Sensitive personal data or information. - Sensitive personal data or information of a person shall include information collected, received, stored, transmitted or processed by body corporate or intermediary or any person, consisting of:

   Password, call data records, etc.

*Researcher’s Suggestion*

This list should be expanded to include information such as sexual orientation, religion and caste. In addition, “electronic communication records” including emails, chat logs and other communications using a computer should be designated sensitive personal information.

ii. **Rule 4** - Body Corporate to provide policy for privacy and disclosure of information.

   (1) The body corporate or any person who on behalf of body corporate collects, receives, possess, stores, deals or handle shall provide a privacy policy for handling of or dealing in user information including sensitive personal information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract. Such policy shall provide for: Type of personal or sensitive information collected under sub-rule (ii) of rule 3; Purpose, means and modes of usage of such information; Disclosure of information as provided in rule 6.
Researcher’s Suggestion

The privacy policy should be made available for view to all individuals to whom the information held by the body corporate pertains. Currently the privacy policy will only be disclosed to the “providers of information” who may not be the individual concerned directly.

iii. Rule 5 – Collection of Information

(1) Body corporate or any person on its behalf shall obtain consent of the provider of the information regarding purpose, means and modes of uses before collection of such information.

Researcher’s Suggestion

Substitution of the term “individual to whom the data pertains” instead of the phrase “provider of the information.”

(2) Body corporate or any person on its behalf shall not collect sensitive personal information unless—the information is collected for a lawful purpose connected with a function or activity of the agency; and the collection of the information is necessary for that purpose.

Researcher’s Suggestion

Suggest a blanket prohibition of collection of biometric data unless a heightened security interest is demonstrated.

(3) While collecting information directly from the individual concerned, the body corporate or any person on its behalf shall take such steps as are, in the circumstances, reasonable to ensure that the individual concerned is aware of.

Researcher’s Suggestion

A simpler phrase like “The body corporate..shall take reasonable steps to inform the individual concerned” instead of the current complex phrasing. Reasonableness has generally been interpreted by courts contextually. For instance, 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.”

120 Gujarat Water Supply and Sewage Board v. Unique Erectors (Guj) AIR 1989 SC 973
(4) Body corporate or any person on its behalf holding sensitive personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

Researcher’s Suggestion

This should be converted into a mandatory obligation to delete or anonymise the information collected within a stipulated period (say 6 months) after the expiry of use for which it was collected.

(6) Body corporate or any person on its behalf shall permit the users to review the information they had provided and modify the same, wherever necessary

Researcher’s Suggestion

Individuals should have the right to review and modify information pertaining to them whether or not they themselves had provided the information to the body corporate. This right should be provided to them wherever the information that pertains to them is incorrect.

(7) Body corporate or any person on its behalf shall provide an option to the provider of the information to opt-in or opt-out.

Researcher’s Suggestion

The wording be changed to “individual to whom the data pertains” instead of “provider of information”.

iv. Rule 6 – Disclosure of Information

(1) Disclosure of information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise.

Researcher’s Suggestion

The wording should be changed to “individual to whom the data pertains” instead of “provider of information

Additional Suggestions

In addition to the following specific comments, we recommend that the Government consider incorporating provisions relating to the following:
i. Mandatory notification of security breach incidents to individuals affected or likely to be affected by such disclosure.

ii. Positive obligation on the body corporates to ensure that information collected is maintained up to date.

iii. Obligation on body corporates to designate a officer to be in charge of responding to privacy complaints from individuals.
CHAPTER – IX

CONCLUSION

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

In the end, the researcher would like to suggest seven broad statutory policy frameworks which should be adopted by the government of India if it is serious in paving a way for a Data protection regime in India. They are-

i. Regulatory requirements - India may adopt a co-regulatory model\textsuperscript{121}, similar to those of both the U.S. and the U.K. However, there must also be sector specific rules. This dual safeguard will place higher standards of protection of data transfer.

ii. Sui generis protection of data - In order to have continued trade with the E.U., it is important that there is adequate legislation in India, which incorporates the eight basic principles that are the essence of the E.U. model. The legislation must provide a minimum standard of protection of data and must establish the basic requirements for compliance with international standards. In order to achieve this, the legislation must address all the terms and concepts relevant in the Indian context, including those of personal and sensitive data, data collector, and rights, duties, and liabilities of the concerned parties.

iii. Specially trained judges - In the field of data protection, there should be a selection of judicial officers specifically trained to deal with intellectual property violations. The Cyber Appellate Tribunal, presently constituted under the IT Act of 2000 is composed of

\textsuperscript{121} Ryan Moshell, And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection, 37.2 Tex. Tech L. Rev. 357 (2004).
only one person who acts as the Presiding Officer of the Tribunal. There must be a provision for engaging an advisor or an independent consultant to adjudicate certain matters before the Tribunal.

iv. Shift from ADR to ODR - The most basic and well advocated solution to enforcement and resolution of the issues is addressing the current court's burden, delay, and costs, and ensuring prompt conclusion of cases with deterrent penalties and compensatory damages. However, this is easier said than done. Steps must be taken to set up an efficient system of Online Dispute Resolution ("ODR"). This would improve access and help trans-border settlement of disputes. A hierarchy of ODR mechanism must be set up on the basis of amount of damages or compensation claimed and/or type of security breach. There must be rules and laws in place with regard to examination of evidence through the electronic medium. Only where the adjudicatory authority feels it absolutely necessary, in the interest of justice, should it recommend the dispute to arbitration or litigation.

v. Data policing - There must be a national set-up for implementation and enforcement of the data protection provisions, examination of crimes related to data, and training in electronic data piracy and enforcement.

vi. Cyber Security Policy - A strong Cyber Security Policy is desirable in India at the wake of the technology revolution by way of the acceptance and adoption of Information and Communication Technology and its benefits. An ideal Cyber Security Policy "presupposes the existence of a sound and secure e-governance" and "the adoption and use of security measures, more particularly, training the judiciary and law enforcement manpower with the knowledge and use of Cyber Forensics and Digital Evidencing."

vii. Law regarding surveillance - Growing awareness for data protection and development of technological systems has led several countries to find it "necessary to draft specific legislative provisions on data protection in the field of video surveillance."

---

126 Giovanni Buttarelli, Protection of personal data with regard to surveillance and Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance, Council of Europe (2000), available at http://www.coe.int/...%20experts/1Report%20Buttarelli%202000.pdf.
is a pertinent caution to avoid either overlapping or rigidity of laws or excessive
generality in the legal framework. India must evaluate and prioritize the effects resulting
from the widespread use of surveillance with regards to citizens' freedom of movement
and behavior.
BIBLIOGRAPHY

BOOKS


ARTICLES

• Kevin Bloss, Raising or Razing the e-Curtain?: The EU Directive on the Protection of Personal Data, 9 Minn. J. Global Trade 645, 645 (2000)


• Vakul Sharma, Legal Issues for Data Protection: Myths and Realities.

OTHER LEGISLATIVE DOCUMENTS