DATA PRIVACY LAW AND GROWTH OF E-COMMERCE: AN INDIAN PERSPECTIVE

Dr. Gargi Rajvanshi*
Mr. Mayank Singhal**

Abstract

Information technology era has made personal information effortlessly accessible, reachable and communicable at a global platform. This junction of swift transfer of such personal information has generated a different set of challenges, which has drastically increased the privacy concern in electronic transactions. Privacy concern is adversely proportionate to the growth of electronic transactions. Forrester Research Institute mentioned that around US $ 15 billion worth of projected e-commerce revenues have be lost by online retailers in 2001 because of customers' privacy concern. Privacy concerns demand adequate legal protection of privacy rights and the data available in online transactions. Hence, this paper projects to examine the adequacy of legal protection of data privacy in India with special reference to growth and fall of e-commerce.

Introduction

In today's scenario internet has enabled the world to communicate and exchange information and data[1] at a swift pace.

* Assistant Director, ICSI, under jurisdiction Ministry of Corporate Affairs, India.

** Vice President, Business Development, Unit Trust of India (MF), Mumbai, Government of India, India.

1 In the usual transactions of the terms, there is an interchange of words "data" and "information." "Data" can be defined as 1) Facts, statistics used for reference or analysis, 2) Numbers, characters, symbols, images etc., which can be processed by a computer, 3) Data must be interpreted, by a human or machine, to derive meaning 4) "Data is a representation of information", 5) Latin 'datum' meaning "that which is given", 6) Data plural, datum singular. "Information" can be defined as 1) Knowledge derived from study, experience (by the senses), or instruction, 2) Communication of intelligence, 3) "Information is any kind of knowledge that is exchangeable amongst people, about things, facts, concepts, etc., in some context," 4) "Information is interpreted data." Data is raw, unorganized facts that need to be processed. Data can be something simple and seemingly random and useless until it is organized. When data is processed, organized, structured or presented in a given context so as to make it useful, it is called Information. If data is at the

The growth of World Wide Web and enabling technologies has made data collection, data exchange and information exchange easier on one shore of advantages of the internet enabled transactions, and on the other shore, this immense exchange, collection, storage and use of information is creating high probabilities of infringement of information privacy. The e-commerce companies, under its 'Infomediary model'[2] collect the data of all the users visiting them and then these companies sell the data to other companies which may further use it for marketing. The company targets the consumers' information for marking and understanding the behavior of their consumers.[3] E-commerce companies are using consumers' and users' personal data to target and track down their market behaviour and for other convert business purposes. Such violation of data privacy is about to cause privacy concern. In business to consumer e-commerce transactions, privacy concern is coming as a vital issue from consumers' as well as from business perspectives. a) From consumers' perspective, e-commerce environment is usually a 'one way mirror effect', where e-commerce businesses ask them to provide their personal information and they are not having even a little knowledge about how their information will be used and protected, b) From business perspective, though collection of personal information is mandatory not only for the completion of transactions but also for understanding consumers' market preferences, yet they are aware of the fact that privacy concern may result consumers' unwillingness to conduct e-commerce transactions and hence may affect the growth of business. Hence under the perspective of data protection, an adequate control mechanism over why, how and what information are collected and used further will not only reduce consumers privacy concern but will advance the growth of e-commerce industry.

---

lowest level in the series, information is placed at the next step. As an example, if you have a list on the Seven Wonders of the World, that is a data; if you have a book giving details about each wonder, it is information. Thus in the context of interchange of data & information, data is a representation of information and information is interpreted data. (May 27, 2015), http://jmcsweeney.co.uk/computing/m150/differences.php.

[2] Under this model of e-commerce companies, the e-commerce sites collect information on consumers and businesses and then sell this information to other companies for marketing purposes.

[3] How to Study your Flashcard, (May 27, 2015) http://flashcarddb.com/cardset/153077-chapter-8-flashcards.

Legal Protection to Data Privacy in E-Commerce: A Need of Hour

The issue of information privacy is vital in e-commerce transactions. According to the definition given by different researchers, (Stone *et al.* 1983[4] Warren and Brandeis 1890[5] Westin 1967[6]) 'Information Privacy' means a concept of controlling how one's personal information is acquired and used.[7] In e-commerce transactions, it seems that consumers are not having control over the collection and use of their information as the websites (firms) collect information without consumers' knowledge and consent in an unauthorized manner with the use of cookies, web bugs etc. This unauthorized access and collection is done with a view to a) capture consumers' need and b) to strategically use the information for website promotion. In e-commerce transactions the major problem is that a) e-commerce companies rely their marketing strategy on consumers' information and their behavior in e-commerce transactions so they are obliged to collect consumers' and visitors' information[8] and b) from consumers view this is invasion of their information privacy or data privacy.[9] Thus collection of information by e-commerce websites on one side and loss of information privacy (i.e. control over the collection, use, storage, processing, dissemination and probable chances of misuse) on other is increasing the privacy concern of the users about protecting their personal information on commercial websites.[10] In an empirical study conducted by Wang and Emurian (2005)[11] it was discovered that 'information privacy concern are the most dreadful obstacle to the persons engaged in e-commerce.' Therefore consumers control over the collection, use and disclosure of personal information tends to reduce their

---

4 Stone, E. *et al.*, *A Field Experiment Comparing Information Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations*, Journal of Applied Psychology Vol. 68 No. 3, 459-468 (1983).

5 Warren, S. & Brandeis, L., *The Right to Privacy*, *Harvard Law Review, Vol.* 4, 193-220 (1890).

6 Westin, A., *Privacy and Freedom*, New York: Atheneum (1890).

7 White, T. B., *Consumer Disclosure and Disclosure Avoidance: A Motivational Framework*, Journal of Consumer Psychology Vol. 14, 41-51 (2004).

8 Bessen, J., *Riding the Marketing Information Wave*, Harvard Business Review Vol. 71, No. 5, 150-160 (1993).

9 Culnan, M. J. & Armstrong, P. K., *Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation*, Organization Science, Vol. 10, No. 1, 104-115 1999.

10 Featherman, M. S. & Pavlou, P. A., *Predicting E-Services Adoption: A Perceived Risk Facets Perspective*, International Journal of Human-Computer Studies, Vol. 59, No. 4, 451-474, (2003).

11 Wang, H. & Emurian, H., *An Overview of Online Trust: Concepts, Elements, and Implications*, Computers in Human Behavior 21, 1, 105-125 (1998).

privacy concern in e-commerce transactions and will support the growth in e-commerce transactions.[12] Legal protection to data privacy may ensure consumer's control over their information and its further use by e-commerce companies. Hence legal protection may go a long way towards ensuring greater individual control over the collection and use of personal information[13] and will improve their participation in e-commerce.

Relationship between Legal Protection to Data Privacy and Growth of E-Commerce

To encounter the challenges of information privacy in e-commerce and to promote legal control over privacy protection in electronic transactions, some legal policies and regulations have already been established at international and national level. At international level, some fair information principles like Notice, Choice, Access, Consent, Enforcement etc. are directed to be followed by the e-commerce companies to ensure the information privacy in the conduct of online transactions. Though at the industry level, even the e-commerce companies are also taking some steps to protect the information privacy of the individuals by adopting and declaring privacy policy, yet much is left to be governed by the nationally and internationally commended regulations. At national level, countries around the world have enacted different laws to protect privacy of individuals. A Business Week/Harris Poll survey[14] found that over 57% of the online buyers want some legal regulations or law to control the use and disclosure of their information by e-commerce websites and to ensure protection of information privacy. Numerous survey[15] conducted by various researchers (Harris Poll Survey, Georgia Institute of Technology survey, Pew Internet and American life etc.) have discovered the fact that consumers as well as businesses want legal protection to regulate protection of personal data and privacy in the regime of e-commerce transactions.

---

12 Stone, E. F. *et al.*, *A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations*, Journal of Applied Psychology, Vol. 68 No. 3, 459-468 (1983).

13 Gray Peter, *Protecting Privacy and Security of Personal Information in Global Electronic Marketplace*, Internet Consumers Organization, Published by Federal Trade Commission (June 24, 2015), http://www.ftc.gov/bcp/icpw/comments/ico2.htm.

14 Harris Poll, Privacy and American Business Press Release (online) (June 24, 2015), http://www.epic.org/privacy/survey/.

15 Harris Poll, Online Privacy: A Growing Threat, Business Week, 96 (2000) (June 22, 2015), http://epic.org/privacy/survey/.

Following are the points that support the need of legal protection to informational privacy in e-commerce transactions:

1) Individuals demand control on data collection and data sharing: Business Week/Harris Poll survey shows that 86% of their respondents want that online businesses should provide consumers with 'opt-in' and 'opt-out' clauses before collecting their personal and sensitive personal information. This supports their demand for consumers' legal control on personal data collection and further sharing of data.
2) Individual desire legal accountability and legal security: Pew and American Life Report[16] (2000 & 2008) showed that 94% of internet users believe that privacy violations should be legally disciplined and they want ability to avail remedies against privacy invasions by online companies.
3) Individual want comprehensive legislation to protect online privacy: Harris Poll survey found that 57% of respondents believe that there should be legal protection to regulate how consumer's personal information is collected and used by online businesses.
4) Individual's value Anonymity: In a number of surveys, conducted by Georgia Institute of Technology's Graphic, Visualization, & Usability (GVU) Center[17] it has been discovered that a majority of individual strongly insist upon and support anonymity in electronic transactions.
5) Individual's opposition to Web Tracking (especially when tracking of personal information is involved): Business Week/Harris Poll (2000)[18] survey found that 89% of their respondents were not comfortable with the online tracking system of online websites and they wanted a restriction to be imposed on the web tracking especially in the tracking of their personal information.
6) Creation of Users' Profile: In a study conducted by the Pew Internet and American Life Project[19] (2000) it was found that 54% of Internet users were objecting to online tracking and they were afraid of the creation of their profile in online transactions. USA Weekend Poll (2000) also

---

16 Report on Trust and Privacy Online: Why American Want to rewrite the rules, Pew Internet and American Life Project. (June 22, 2015), http://www.pewinternet.org/reports/toc.asp?Report=19.

17 Survey Report (June 22, 2015), http://www.cc.gatech.edu/gvu/user_surveys/survey-1998-04/graphs/#privacy.

18 Public Opinion on Privacy, (June 22, 2015), http://epic.org/privacy/survey/.

19 *Ibid*

showed that 65% of respondents thought that tracking computer usage and creation of users' profile in internet was an invasion of privacy.

7) Lack of Individuals' trust in e-commerce transactions (about the administration of their personal information/data) and apprehension about the abuse of privacy: A survey conducted by American Society of Newspaper Editors on privacy concern (2000)[20] showed that 51% of respondents strongly felt that online companies might violate their personal privacy and same study showed that 52% of the respondents were having 'no confidence at all' in the online company that they use the personal information of their consumers exactly in the same way which they had said they would.
8) Individuals' demanded adequate legal protection for privacy protection in electronic transactions: As per Harris Poll survey (2002)[21] 83% of respondents themselves asked online companies to remove their names, addresses and other personal information fearing the loss of their personal information and consequently invasion of their privacy rights in online transactions. This shows that consumers do not trust the industry policies for the adequate protection of their personal data, and therefore demand adequate legal protection to protect online privacy in online transactions.
9) Individuals' Right to Awareness: A study conducted by Pew Internet and American Life Project, showed that 56% of Internet users are unaware and unknown about installation and use of cookies and more sophisticated tracking tools, such as 'web bugs' or 'spyware' by online business to access and collect consumers' personal information and thereafter tracking their online behavior. Hence if awareness about the unauthorized tracking of information and legal control over such tracking are provided, consumers will be more willing to provide their personal information in e-commerce transactions.

From the above discussions it can be assumed that a) consumers are not having control over the access, collection, use and disclosure of their personal information, b) since consumers are not having control on the manner of collection and use of their

---

20 *See* Public Opinion on Privacy (June 18th, 2015), http://epic.org/privacy/survey/.

21 Harris Interactive, 2002, The Harris Poll #46, September 10, 2002, http://www.harrisinteractive.com/harrispoll/index.asp?PID=325.

information this enhances consumers potential risk of the invasion of their privacy rights in the conduct of electronic transactions, c) they are sincerely concerned about their privacy protection in e-commerce transactions, d) consumer privacy concerns may create their unwillingness to participate in e-commerce transactions e) people want legal control over their privacy invasion and f) in the absence of any legal control over the privacy issues, the consumers themselves tends to take self regulatory mechanism to protect their privacy in e-commerce transactions. For instance, according to the survey conducted Harris Poll designed by Privacy & American Business and sponsored by Microsoft in June 2004,[22] in the lack of legal protection against the invasion of privacy rights in e-commerce, a) Two-thirds of Americans had taken various steps to protect their privacy; including deciding not to shop at a store or requesting that a company removes personal information from a database. b) 87% indicated that they had asked a company to remove their information from a marketing database. c) 60% decided not to patronize a store because of doubts about the company's privacy protections. d) 65% had declined to register at an e-commerce site because of privacy concerns.

Consequently, it can be assumed that adequate legal protection over privacy concern and information privacy will ensure individuals' about the protection of their privacy rights in e-commerce transactions. This will further support their willingness to conduct e-commerce transactions and thus will support a) protection of personal data on one hand and b) growth of e-commerce on other hand.

Data Privacy in E-Commerce: Indian Legal Perspective

In the information and communication technology equipped society, the term privacy is closely connected to data protection.[23] Individual's data like his name, telephone numbers, profession, family, choices, pan card number, credit card details, social security number etc. are disclosed in the electronic transactions and then are available on various websites.[24] Though the

---

22 New National Survey on Consumer Privacy Attitudes, Privacy & American Business Landmark Conference, Privacy and American Business Press Release, (June 10, 2004) (June 22, 2015), http://epic.org/privacy/survey/.

23 Philip E. Agre & Marc Rotenberg, Technology and Privacy: The New Landscape, Massachusetts Institute of Technology Press. USA. (1997) (May 27, 2015), http://polaris.gseis.ucla.edu/pagre/landscape.html

24 Miriam J. Metzger, *Privacy, Trust and Disclosure: Exposing Barriers to Electronic Commerce*, Journal of Computer Mediated Communication, Vol. 9

authorized collection and the storage of data may only create probability of the loss of information privacy[25] but the unauthorized access, collection, use, misuse, relocation and transmission of the information to the third party essentially result in the intrusion of information privacy of the individuals. Hence improper control on transmission of information can be the root cause for privacy challenges in electronic transactions. Law will not only determine a) what privacy entails, b) how it is to be valued, and c) to what extent it should be endowed with legal protection, but also ensures authorized protection to the circumstances under which individuals can value their privacy and protect it from the violation of unauthorized intrusion by others. Knight Bruce in *Prince Albert* v. *Strange*[26]upheld that a third party intrusion into one's privacy results in grave violation of right to privacy and hence implies need of legal protection to right to privacy.

Under this state of affairs with the growing requirement of protecting information privacy in electronic transactions, various countries have introduced special legal framework[27] to protect data privacy in electronic transactions. In the Indian context, though it would be a misnomer to say that India does not have legislation to encounter the challenges of cyberspace, yet the fact is that in the absence of any specific legislation, protecting of information privacy and data privacy in e-commerce transactions seems dicey and distort. To counter the challenges of information and communication technology, the Indian Legislature has enacted Information Technology Act, 2000, Information Technology (Amendment) Act, 2008 and others too, but challenges of information privacy and data privacy are not addressed in an exclusive and specific manner. India is not having a comprehensive legislative framework to deal specifically with privacy issues in electronic transactions.[28] The Information Technology Act, 2000 was enacted chiefly to facilitate e-commerce;

No. 4, (2004) (May 27, 2015).

25 Information privacy is synonym to data privacy. Information Privacy or data privacy is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them. (May 27, 2012), http://en.wikipedia.org/wiki/Information_privacy.

26 *Prince Albert v Strange* (1848) 2 De G & SM 652, 698; 64 ER 293, 314.

27 *See* UK Data Protection Act (DPA), 1998, US Electronic Communication Privacy Act (ECPA), 1986.

28 Shrikant Ardhapurkar *et al.*, *Privacy and Data Protection in Cyberspace in Indian Environment*, International Journal of Engineering Science and Technology, Vol. 2 No. 5, 942-951(2010).

hence privacy is not a prior concern of the Act.[29] Now the questions for analysis are that a) in what way Indian legal framework is promoting data protection and data privacy and 2) if it provides some legal protection to data, how far it is effective[30] in protecting personal data and privacy in electronic transactions.

1. Information Technology Act, 2000 and Data Privacy: An Analysis

Indian legislature has enacted Information Technology Act, 2000 for the purpose of complying with the requirements of UNCLTRAL (United Nations Commission on International Trade Law), adopted model law[31] on electronic commerce[32] on one stand,[33] and for providing legal recognition to the transactions carried out by the means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce.[34] Accordingly the Act bought into existence for following reasons:[35] 1) To facilitate the development of e-commerce transactions, 2) To ensure the regulatory environment for the security of e-commerce transactions, 3) To provide legal structure for governing electronic contracts, security and integrity of electronic transactions. (This legal structure will directly relate to the growth and development of e-commerce), 4) To facilitate and validate the use of digital signatures for authenticating the electronic records, 5) To facilitate the growth of Indian IT sector across the globe, 6) To ensure the safety and security of electronic

---

29 Mathur, S. K., *Indian Information Technology Industry: Past, Present and Future A Tool for National Development*, Journal of Theoretical and Applied Information Technology. (2006). (Online) (May 28, 2015), http://perso.univ-rennes1.fr/eric.darmon/floss/papers/MATHUR.pdf.

30 Naavi Report on Cyber Laws for CxO: Be Aware, Be empowered, Ujvala Consultants Pvt. Ltd., (2010) Effectiveness of any legislation is measured by the ease with which the intended beneficiary of the legislation can invoke legal remedies and obtain relief.

31 UNCITRAL Model Law on Electronic Commerce, Guide to Enactment with 1996 (May 27, 2015), http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf.

32 UNCITRAL Model Law on Electronic Commerce, Guide to Enactment with 1996 (May 27, 2015), http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf.

33 The Information Technology Act, 2000 (May 26, 2015), http://en.wikipedia.org/wiki/The_Information_Technology_Act,_2000.

34 The Information Technology Act, 2000, (May 26, 2012), http://www.aicte-india.org/downloads/itact2000.pdf.

35 Nasir M. Ali, *Legal Issues involved in E-commerce*, Ubiquity (Mazgine), New York, NY, USA (2004) (May 28, 2015), http://ubiquity.acm.org/article.cfm?id=985607.

transactions, and 7) To attract Foreign Direct Investment (FDI) in Information Technology sector.

Under the regime of privacy rights, every individual wants to keep his or her personal affairs to himself, but in the electronic transactions, variety of individual's information are collected and stored, which can easily make others to identify that individual. Databases collected in the online transactions, where cross-matched can easily create profile of the individuals and can predict their behavior. This involves the sheer violation of data privacy in electronic transactions. The provisions of the Act for the purpose of data protection and control over disclosure, collection, storage and misuse of the information in electronic transactions can be examined as follows:

(A) Provisions pertaining to data[36] protection & personal data[37] protection

In Information Technology, Act, 2000, no such concept as 'personal data' has been discussed. It defines 'data'[38] but does not provide any definition of personal data. Furthermore, the definition of data is provided with more relevancies to

---

36 Data means information which (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by Section 68, or(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d). Source: Information Commission Office, Government of United Kingdom, (May 29, 2015), http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx.

37 Personal data means data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and (c) includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. Source: Information Commission Office, Government of United Kingdom, (May 29, 2015) http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx

38 Section 2 (o) of IT Act, 2000 'data' means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer; (May 29, 2015), http://eprocure.gov.in/cppp/sites/default/files/eproc/itact2000.pdf.

cybercrime.[39] Hence, there is confusion among the researchers whether the Indian IT Act, 2000 deals with data protection' or with 'personal data protection' as well.

(B) Civil Liability in case of data, computer database theft, privacy violation etc[40]

The Information Technology Act, 2000 has devoted Chapter IX on the cyber contravention. Section 43 (a) to 43 (h) has enlist wide range of cyber contraventions related to unauthorized access to computer, computer system, computer network and resources. Section 43 of the Act[41] covers various issues, which create civil liability against the wrongdoer and provides for damages (not exceeding one crore rupees) to the person so affected from the defined instances. These instances include:

(a) Computer trespass, violation of privacy etc.
(b) Digital copying, downloading and extraction of data, computer database or information; theft of data held or stored in any media
(c) Data Contamination, computer disruption etc.
(d) Data loss, data corruption etc.
(e) Computer data/database disruption, spamming etc.
(f) Denial of service attacks, data theft, fraud, forgery etc.

It is noteworthy that compensation for these entire categories of cyber contravention can be awarded only when any one is affected with such access, disruption, denial etc. What, if the data subject is not effected out of any unauthorized access but such access has caused the violation of his privacy rights.

(C) Criminal Liability in case of data, computer database theft, privacy violation etc[42]

The IT Act, 2000 also provides (vide Chapter XI) for defining and creating liability for cyber offences. Sections 65 to 74 of the Act cover a wide range of cyber offences related to unauthorized alteration, deletion, addition, modification, alteration, destruction,

---

39 The Final Report: The First Analysis of the Personal Data Protection Law in India, Prepared by CRID-University of Namur, Report delivered in the framework of contract, JLS/C4/2005/15 between CRID and the Directorate General, Justice, Freedom and Security. (May 29, 2015), http://ec.europa.eu/justice/data-protection/index_en.htm.

40 Sharma, Vakul, Information Technology-Law & Practice, Delhi: Universal Law Publishing Co. Pvt. Ltd (2004)

41 Section 43 of Information Technology Act, 2000: Penalty for damage to computer, computer system, etc. (May 29, 2015), http://eprocure.gov.in/cppp/sites/default/files/eproc/itact2000.pdf.

42 Sharma, Vakul, Information Technology-Law & Practice, Delhi: Universal Law Publishing Co. Pvt. Ltd, 2004.

duplication or transmission of data, and computer database. Some provisions deal with the data related offences, like Section-65 related to 'Tempering with the computer source' which was not limited to the protection of computer source code but was extending safeguards for computer data base from unauthorized access. Section 66 (Hacking with Computer system), was also indirectly protecting data from unauthorized access and misuse. According to Mr. Unni, unauthorized access to any information diminishes its value/utility and hence injures the confidentiality of a document.[43] For example if any sensitive personal information is transmitted in e-mail or saved in an e-mail, or in computer and if any person accesses the said document without any authority, than the value of the information is completely lost and it will result in loss of personal data and will make the accessing party liable under Section 66. It is noteworthy that to make a person liable under Section 66, his mens rea or guilty intention to cause such access has to be proved.

It is noteworthy that out of various provisions dealing with cyber offences, it was only Section 72[44] of the Act, which was specifically directed at the protection of confidentiality and privacy. Section-72 aimed at the protection of privacy and confidentiality from public (and private) authorities,[45] which have been granted power under the provisions of Information Technology Act, 2000 to secure access to any electronic record, book, register, correspondence, information, document or other material information. The purpose of incorporating this section was to ensure that the person who is legally entitled to secure an access to any information[46] shall not take unfair and unmerited

---

43 V.K. Unni, *Internet Service Provider's Liability for Copyright Infringement-How to clear the Misty Indian Perspective,* 8 Richmond Journal of Law & Technology. Vol. 13 (2001) (May 29, 2015), http://jolt.richmond.edu/v8i2/article1.html.

44 Section 72 of Information Technology Act, 2000: Penalty for breach of confidentiality and privacy: Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book. register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. (May 29, 2012), http://eprocure.gov.in/cppp/sites/default/files/eproc/itact2000.pdf.

45 These public and private authorities may be referred as 'data collectors' or 'data users'.

46 Persons conferred under the Act : The Act has conferred powers to : a)The Controller of Certifying Authorities (Ss. 17-18) b) The Deputy and Assistant

advantage of such information by disclosing it to any unauthorized third party without seeking due consent. This section creates an obligation of confidence between the 'data collectors' and a 'data subject'. Section 72 has a limited appliance, as it is applicable only to the persons who have gained access to the information under some authorized channel and not to the unauthorized access of personal information by available means.[47]

(D) Information Technology Act, 2000 vis-à-vis Data Privacy: A Critique

From the above discussion, it can be submitted that Information Technology Act, 2000 is not data protection legislation per se. The Act does not lay down any specific provisions for data protection and privacy protection; even no such term as 'personal data' is defined in the Act. The IT Act, 2000 is a common legislation, which articulates on various subject matters that involves digital signatures, public key infrastructure, e-governance, cyber contraventions, cyber offences and confidentiality and privacy. This lack of specific provisions under IT Act, 2000 is hardly favourable to an effective protection of data and privacy in electronic transactions.

In comparing the Indian legislative framework with the global standards on the protection of personal data and privacy in electronic transactions like European Directives on Data Protection (EC/95/46), OECD guidelines on Protection of Privacy and Tran border Flow of Personal Data, 1980 and the Safe Harbor principles of US, it can be argued that the issue of data protection and privacy was dealt in a piecemeal manner under Information Technology Act, 2000. There is no legal framework specifically dealing with data protection authority, data quality, proportionality of data collection, data transparency, etc. According to Vakul Sharma, even after the inclusion of the proposed amendments in IT Act, 2000 suggested by the Expert

---

Controllers of Certifying Authorities (Ss. 17 and 27) c)Licensed Certifying Authorities (S. 31) and Auditors (Rule 312) d) The Adjudicating Officer (S 46) e) The Presiding Officer of the Cyber Appellate Tribunal (Ss. 48-49) f) The Registrar of the cyber Appellate tribunal (S. 56 and rule 263) g)Network Service provider (S. 79) h) Police Officer (Deputy Superintendent of Police) (S. 80) (May 29, 2015), http://www.legalserviceindia.com/article/l288-Breach-of-privacy-&-Confidentiality-.html.

47 Salim Nimitha, *Breach of Privacy and Confidentiality under the Information Technology Act, 2000*, Legal Service India, (2009) (May 29, 2015), http://www.legalserviceindia.com/article/l288-Breach-of-privacy-&-Confidentiality-.html

Committee, there will be lack of appropriate legal framework for data protection and privacy in India.[48] He has suggested the incorporation of a new and a purpose-specific legislation for ensuring appropriate data protection and privacy in information technology era.[49]

(E) Proposed Amendments in the Information Technology Act, 2000 vis-à-vis Data Protection and Data Privacy

Numerous researchers[50] were of the opinion that the Information Technology Act, 2000 in India does not contain sufficient provisions for data protection. The Indian government was aware of the lack of the regulation in this field, but after the analysis of different researches in India and abroad, the Indian Government appointed an Expert Committee[51] on Cyber Law to analyze the position of Indian legislation on the protection of personal data and to suggest amendments to the Information Technology Act, 2000.[52] The expert committee was formed with the essential objective 'to consider and recommend suitable legislation for data protection (privacy) in the Information Technology Act, 2000.' The Expert Committee in its report[53] was of the view that Sections 43, 65, 66 and 72 should be amended for the purpose of 'data protection and privacy.'[54] They recommended that in addition to the contractual responsibilities between the parties, Sections 43,

---

48 Sharma Vakul, Information Technology-Law & Practice, Delhi: Universal Law Publishing Co. Pvt. Ltd, 2004.

49 Subramanian Ramesh, *Security, Privacy and Politics in India: A Historical Review*, 8th Annual Security Conference Disclosure in Security, Assurance and Privacy, Las Vegas, NV, USA, 15-16, (2009).

50 Jamil & Khan, *Data Protection Act in India Compared to The European Union Countries*, International Journal of Electrical and Computer Sciences IJECS-IJENS Vol. 11 No. 06; Parag Diwan and Shammi Kapoor, Cyber and e-commerce laws, 4 (2nd ed.2000); Jon Bing, Data Protection: Jurisdictions and the Choice of Law; Kuner Christopher, *Data Protection Law and International Jurisdiction on the Internet*, International Journal of Law and Information Technology, Vol. 18, Issue 2, 176-193, Oxford University Press.

51 Notification no. 9(16)/2004-EC, January 7, 2005.

52 Nair Latha R, *Does India Needs A Separate Data Protection Law?* World Data Protection Report, Vol. 5 No. 12, (2005) (May 29, 2012), http://www.knspartners.com/files/BNA%20Article-180106.pdf.

53 Department of Information Technology (August 2005).

54 Blok, P., Recht on Privacy, Boom (2002): In Blok's words privacy can be as: The individual right to privacy both safeguards an undisturbed private life and offers the individual control over intrusions into his private sphere. Given this definition, the boundaries of the private sphere are central to the meaning of privacy. The right to privacy guarantees individual freedom within the home, within the intimate sphere of family life, and within confidential communication channels. In combination with physical integrity, these 'privacies' form the core of the legally protected private sphere. (May 26, 2013), http://www.law.ed.ac.uk/ahrc/script-ed/vol4-4/cuijpers.pdf.

66 and 72 of Information Technology Act, 2000, should be revisited and revised with following amendments:

1. That under Section 66, there should be a classification of offences according to the fraudulent and dishonest nature of offence and punishment should be awarded in accordance with the gravity of the offence,
2. That there should be an inclusion of a new Section 43 (2) defining and protecting 'Sensitive Personal Data' and other information ensuring reasonable security practices and procedure thereto,
3. That under Section 43 (2), body corporate should be endowed with an additional responsibility of ensuring security of sensitive personal data of their consumers. With this, two explanations defining 'Reasonable Security Practices and Procedures'[55] and 'Sensitive personal data or information'[56] has been recommended,
4. That Section 43(2) should be read with the explanations defining reasonable security practice and procedures and sensitive personal data or information. This crucial initiative behind the proposed amendment was to grant statutory protection to sensitive personal data or information.[57] The proposed amendment is providing obligation on the body corporate to adopt and implement reasonable security practices and procedures to promote protection to sensitive personal data, stored in their computer, computer source etc.
5. That the adoption of reasonable security practices and procedures for the protection of sensitive personal data or information will amounts to 'self regulation',
6. That Section 72 should be amended with the aim of extending data protection against disclosure of personal information by the

---

55 Section 43, Explanation (v) "Reasonable security practices and procedures" means, in the absence of a contract between the parties or any special law for this purpose, such security practices and procedures as appropriate to the nature of the information to protect that information from unauthorized access, damage, use, modification, disclosure or impairment, as may be prescribed by the Central Government in consultation with the self-regulatory bodies of the industry, if any.

56 Section 43, Explanation (vi): Sensitive personal data or information" means such personal information, which is prescribed as "sensitive" by the Central Government in consultation with the self-regulatory bodies of the industry, if any.

57 The Final Report: First Analysis of the Personal Data Protection Law in India, CRID-University of Namur: This crucial initiative behind the proposed amendment was to grant statutory protection to sensitive personal data or information. (May 30, 2015), http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_india_en.pdf

'intermediaries' (network service providers) without one's consent.[58] Such intermediaries must compensate for violation of data privacy by their unauthorized access and disclosure of data.

2. Information Technology (Amendment) Act, 2008

The need to facilitate the protection of data privacy and growth of e-commerce hand in hand has called for the amendments in the Information Technology Act, 2000. This has resulted into the enactment of the Information Technology (Amendment) Act, 2008. The Information Technology (Amendment) Act, 2008 has been enacted to facilitate and legalize e-commerce transactions, e-fund transfers, e-storage of data, e-filling of documents with the Government departments on one side and to increase the protection of personal data and information for national security, countries' economy, public health & safety on the other.[59] Though the Indian Information Technology (Amendment) Act, 2008 is not a privacy law, it encloses some provisions which address challenges of data protection including privacy in e-transactions.[60] Section 43A of this Act directs that all body corporate,[61] which are in possession of data and information of their consumers in their computer source, will implement 'reasonable security practices[62]' to prevent the unauthorized access to the personal data of their consumers. This section further entails that failure to protect the sensitive personal data of the individuals during the processing period by the company will make company liable to compensate the aggrieved person, whose personal data is so compromised. While explaining Section 43 A of IT (Amendment Act), 2008,

---

58 Mohammed Nyamathulla Khan, Does India have a Data Protection Law, Legal Service India (2009) (28th April 2015), http://www.legalserviceindia.com/article/l406-Does-India-have-a-%20Data-Protection-law.html.

59 Workshop Report, National Seminar on Enforcement of Cyber law, New Delhi, (May 8, 2010) (May 27, 2015) http://catindia.gov.in/pdfFiles/IT_Act_2000_vs_2008.pdf.

60 Bajaj Kamlesh, (CEO, DSCI), A Report of Data Protection-Security and Privacy, Information Technology Laws Workshop, Delhi University, 19-21 March, 2010.

61 Section 43 A, Explanation (i) 'body corporate' means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.

62 Section 43 A, Explanation (ii) 'reasonable security practices and procedures' means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

Kamlesh Bajaj[63] has detailed that the company will be liable for the loss of data during its processing at company's end and the company cannot take any excuse from their responsibility on the ground that there was no negligence on the part of the company in implementing or maintaining reasonable security practices. He further explained that reasonable security practices and procedure will constitute practices and procedures to protect information from unauthorized access, damage, use, modification, disclosure or impairment as may be specified in an agreement between the parties or as may be specified in any law in force. In the absence of any such agreement or law, the central government will prescribe the security practices and procedure in consultation with professional bodies and associations.[64]

The penalty under Section 72 of IT Act, 2000 for the disclosure of information was restricted only to those who are legally authorized to secure access to an electronic record and document under the act, and hence Section 72-A[65] has been incorporated in IT (Amendment) Act, 2008, which provides liabilities of intermediaries and other persons for breach of privacy and confidentiality under lawful contract. Section 72-A[66] reads that save as otherwise provided in this Act or any other law for the time being in force, (i) any person including an intermediary who; (ii) while providing services under the terms of lawful contract; (iii) has secured access to any material containing personal information about another person; (iv) with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain; (v) discloses; (vi) without the consent of the person concerned, or in breach of a lawful contract; (vii) such material to any other person; and (viii) shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both. Apart from Sections 43A and 72A, there are some other provisions as well which though not specifically but in one way or other tackle the challenges of data protection and data privacy. These provisions are:

1. Section 66 – Computer Related Offences
2. Section 66A – Punishment for sending offensive messages through communication service, etc.
3. Section 66B – Punishment for dishonestly receiving stolen

---

63 CEO of Data Security Council of India, 2009.

64 Explanation (ii) of Section 43A of Indian Information Technology (Amendment) Act, 2008.

65 Penalty for breach of confidentiality and privacy.

66 Section 72A: Punishment for disclosure of information in breach of lawful contract.

computer resource or communication device.
4. Section 66C – Punishment for identity theft
5. Section 66D – Punishment for cheating by personation by using computer resource
6. Section 66E – Punishment for violation of privacy
7. Section 66F – Punishment for cyber terrorism
8. Section 67 – Punishment for publishing or transmitting obscene material in electronic form
9. Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form
10. Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form
11. Section 67C – Preservation and Retention of information by intermediaries
12. Section 69 – Power to issue directions for interception or monitoring or decryption of any information through any computer resource
13. Section 69A – Power to issue directions for blocking for public access of any information through any computer resource
14. Section 69B – Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security
15. Section 79 – Exemption from liability of intermediary in certain cases
16. Section 84A –Modes or methods for encryption
17. Section 84B –Punishment for abetment of offences
18. Section 84C –Punishment for attempt to commit offences

3. Critical Analysis of Information Technology (Amendment) Act: 2008

1) Section 43A does not mention anything about 'Personally Identifying Information'. Data protection legislation should cover within its sphere all types of personally identifying information which either by itself or in combination with other information help in identifying or creating the personal profile of an individual.
2) Lack of adequate extra-territorial jurisdiction: In the present scenario the provisions of data protection and privacy protection are devoid of effective extra-territorial

application. Though Section 75[67] of the Act provides for the extra-territorial applicability of the Act, yet is subject to the restriction that the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.[68] Section 43A and 72A do not specifically talk about the extra-territorial applicability for protection to data and privacy in information technology era. Hence, where data is transferred outside the territories of India, there exist no legal protection to data privacy in electronic transactions.[69]

3) Under IT (Amendment) Act, 2008, neither the term 'personal information' is defined at all, nor has 'sensitive personal information' been visibly defined. The absence of a clear definition of personal information may imply that there is no difference between the traditional definition of personal information[70] and sensitive personal information.[71]
4) IT (Amendment) Act, 2008 provides 'civil remedy' under Section 43A to the body corporate a) for negligence in implementing 'reasonable security practices and procedures', b) while handling 'sensitive personal data and information', c) resulting in wrongful loss or wrongful gain to any person. This shows that the civil remedy in IT

---

67 Sec 75 Act to apply for offence or contraventions committed outside India: (1) Subject to the provisions of sub-Section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality. (2) For the purposes of sub-Section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

68 Jacob Shojan, *Data Protection Law in India*, The Indlaw Online Journal (2009), (May 31, 2012),http://www.indlaw.com/Updates/EditorsPick.aspx.

69 *See* Amrik Singh Juneja v. State of Punjab and Another, (Decided February 14th, 2013), High Court of Punjab & Haryana, CRM-M No. 23026 of 2012.

70 Personal data means data which relate to a living individual who can be identified: (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, (c) and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

71 Sensitive personal data means personal data consisting of information as to: (a) the racial or ethnic origin of the data subject, (b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), (e) his physical or mental health or condition, (f) his sexual life, (g) the commission or alleged commission by him of any offence, or (h) 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.

(Amendment) Act, 2008 can be claimed only when there is a) negligence of the body corporate and b) if causes wrongful loss and wrongful gain to others.[72]

5) The Act provides for the criminal punishment for a person if (a) he discloses sensitive personal information; (b) does so without the consent of the person or in breach of the relevant contract; and (c) with an intention or knowledge that the disclosure would cause wrongful loss or gain. It means criminal remedy can be availed only when disclosure of sensitive personal information is done with an intention of or knowledge of causing wrongful loss or wrongful gain. Hence the innocent violation of one's privacy even with major injury to the information holder will be out of criminal application under the Act.
6) Information Technology Act, 2000 provided[73] a ceiling on the compensation (INR one crore) under Section 43 and Section 43A (INR five crore), but in IT (Amendment) Act, 2008,[74] no upper limit is provided for the compensation under Section 43 and 43A. According to Karnika Seth,[75] the deficiency of not providing ceiling on the compensation amount in Sections 43 and 43A in IT (Amendment) Act, 2008 is seen to be abused and misused in the instances where the companies are filing the frivolous claims against their ex-employee, who may have joined some competitor firm, without breaching their employment contract.
7) Section 72A criminalizes the breach of confidentiality and privacy, but in the cases where criminal penalty cannot be awarded for violation of privacy and confidentiality, no remedy is available in any form of compensation to the victims of such breach of confidentiality and privacy.

---

72 It shows that to avail the protection under Section 43A, the person whose sensitive information is being criticized has to prove either wrong loss to him or wrongful gain to others.

73 Section 43: Damages by way of compensation not exceeding one crore rupees to the person affected by damage to computer, computer system, computer network, computer resource etc. and Section 43A: Damages by way of compensation, not exceeding five crore rupees, to the person affected by the failure of body corporate to protect their data and information.

74 Information Technology (Amendment) Act, 2008, Department of Electronics and Information Technology, Ministry of Communication & Information Technology, Government of India (June 2, 2015), http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf.

75 Seth Karnika, *Information Technology Act, 2000 vs.2008: Implementation, Challenges, and the Role of Adjudicating Officers*, National Seminar on Enforcement of Cyber law, New Delhi, India (2010) (May 2, 2015), http://catindia.gov.in/pdfFiles/IT_Act_2000_vs_2008.pdf.

8) Section 72A seems to be narrowly drafted as it only deals with the information, which is obtained in a contractual relationship between the parties. According to a survey conducted by Business Week[76] various personal information of individuals are collected by tracking their online behavior. Hence there is lack of legal protection for the information which are collected without authority and then compromised towards the violation of data privacy in electronic transactions.
9) With the preceding discussion, it can be alleged that Section 43A and 72A of IT Act, 2008 do not comprehensively address the challenges of data privacy in electronic transactions in India.[77]
10) IT (Amendment) Act, 2008 has been enacted with expectation of providing an effective protection to data and privacy in electronic transactions, but an analysis of IT (Amendment) Act, 2008 and its corresponding rules[78] articulates that the provisions for data protection and privacy protection are very limited in its scope for civil penalties for failure to protect personal data and civil and criminal penalties for the disclosure of information without consent or in breach of contractual obligations.[79] To strengthen the provisions of data protection and privacy protection in electronic transactions, Indian Government introduced Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.[80] These new rules regulate the

---

76 Privacy on the Net, A Growing Threat, Business Week/Harris Poll, (March, 2000) (March 14th, 2015), http://www.businessweek.com/2000/00%2012/b3673006.htm.

77 Mathias Stephen, *Indian Privacy law*, (Online) Outsourcing Law, (2011) (June 1, 2015), http://www.outsourcing-law.com/jurisdictions/countries/india/india-privacy-overview/2011-indian-privacy-law/.

78 *See* 1) Information Technology Rules (Procedure and safeguards for interception, monitoring and decryption of Information) rules, 2009, 2) Information Technology Rules (Procedure and safeguards for blocking for access of information by public) rules, 2009, 3) Information Technology Rules (Procedure and safeguards for monitoring and collecting traffic data or Information) rules, 2009 (June 1, 2012), http://www.mit.gov.in/content/notifications.

79 Hawkins Chris, *Indian Data Privacy Rules-Impact of Recent Changes* (Online) Mondaq's Newsletter on Information Technology and Telecoms (2011) (June 1, 2015) http://www.mondaq.com/x/145704/Data+Protection+Privacy/Indian+Data+Privacy+Rules+Impact+Of+Recent+Changes.

80 Related to Section 43A and 79 of the IT (Amendment) Act, 2008 (With effect from April 13, 2011).

collection, disclosure, transfer and storage of sensitive personal data and has widened the scope of regulations mentioned in Section 43A of Information Technology (Amendment) Act, 2008.

Consequently, it can be concluded where there were no provisions for data protection in electronic transactions at that point of time Information Technology (Amendment) Act, 2008 seems to provide a framework related to data protection in electronic transactions. The Act does not specifically address the challenges of data protection and data privacy in electronic transactions. Various researchers[81] marked that presently India is one of the few countries, which do not have created any sector specific legislation to standardize collection, use, control, utilization, and appropriate disposal of data collected in electronic transactions. Hence to ensure data protection with facilitation for growth of e-commerce transactions a 'sector-specific' law is need of the hour in global perspective.

4. Other Statutes on Data Protection in Electronic Transactions

Apart from Information Technology Act, 2000 and Information Technology (Amendment) Act, 2008, there are following statutes as well which affords some indirect protection to data and privacy:

1. Indian Penal Code, 1860[82]
2. Indian Telegraph Act, 1885[83]
3. Indian Contract Act, 1872[84]
4. Indian Copyright Act, 1957[85]

---

81 *See* Vinita Bali, *Data Privacy, Data Piracy: Can India Provide Adequate Protection for Electronically Transferred Data?* Temple International & Comparative Law Journal, Vol. 21, No. 103, 111-113 (2007).

82 The IPC, 1860 does not directly address the breach of data privacy but has been used to bring prosecutions for data theft under Section 405 (criminal breach of trust), 406 (Punishment for criminal breach of trust), 420 (cheating and dishonesty including delivery of property).

83 This Act protects the personal information and privacy of individuals in the telecommunication area.

84 The Indian Contract Act renders data protection and privacy protection in the form of breach of contract and specific performance of contract. The law of contract says that the parties involved in a contract must adhere with the rules and regulations as specified in the agreement. If terms & conditions calling for the protection of information are violated by the disclosure of the information shared between the parties, causing intentional damages to other amounts to breach of contract.

85 This Act provides security to literary, artistic, dramatic and musical work. The copyright act provide right to the original author of above mentioned fields so that no one can misuse their work and maintain the privacy if it is related with

5. The Specific Relief Act, 1963[86]
6. The Public Financial Institution Act, 1983[87]
7. The Consumer Protection Act, 1986[88]
8. The Credit Information Companies (Regulation) Act, 2005[89]

5. Data Protection Rules, 2011: Critical Analysis

Information Technology Act, 2000 with its Amendment in 2008 does not seem to have an effective address to the concern of data protection and privacy security in the electronic transactions.[90] After considering an elongated demand from the individuals' to enact a specific legislation to protect their personal information and privacy in electronic transactions, Indian Government has notified the 'Information technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011' (Here after referred as Rules) under Section 43A of Information Technology (Amendment) Act, 2008.[91] These rules were notified to support and further Section 43A of the Act, for protecting individuals' data in electronic transactions. The aim of these 'Rules', is to provide a strong privacy law for the protection of personal data and privacy in electronic transactions.

Salient features of Information technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

1) These rules have addressed the law relating to information

---

some sensitive information and maintain the originality of work. Specifically mention Section 16 and 63B of Indian Copyright Act, 1957.

86 This Act provides for the specific relief to the people, who can claim temporary and permanent injunctions against unauthorized disclosure of confidential information.

87 *Kottabomman Transport Corporation Limited v. State Bank of Travancore and Others*, AIR 1992 Ker. 351: Banks are under a duty to secrecy and not to disclose information to third party.

88 This Act provides the provisions through which the consumer can claim protection from exploitation and can save them from deficiency of services by disclosing proprietary information, personal information etc. without adequate authorization.

89 *See* Section 19: Information should be accurate and protected against unauthorized use and disclosure.

90 Khan M., *Does India have a Data Protection Law?* (Online) Legal Service India (June 2, 2012), http://www.legalserviceindia.com/article/l406-Does-India-have-a-Data-Protection-law.html.

91 Information technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Notified by Ministry of Communication and Information technology, Department of Information Technology (11th April, 2011).

in general, where personal information and sensitive personal information are specifically defined and addressed. 'Sensitive Personal Information' is specifically defined in Rule 3 as sensitive personal data or information of a person relating to: (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, with an exception that an information a) that is freely available or accessible in public domain or b) is furnished under Right to Information Act, 2005 or any other law for the time being in force, shall not be regarded as sensitive personal data or information for the purpose of these rules. It has to be noted here that the sensitive personal information in these rules[92] deals only with the information of individuals and not the information of businesses.

2) Privacy Policy:[93] The Rules provide that a) each body corporate is required to frame the privacy policies and to publish them on its website. Apart from this the body corporate is b) required to appoint a grievance officer.[94] c) The privacy policy required under rule 4 must describe i) what information are collected, ii) what is the purpose for which they are collected, iii) to whom and how the information might be disclosed and iv) the reasonable security practices followed by the body corporate to safeguard the information. d) It is mandatory for body corporate to publish 'privacy policy' irrespective of the fact whether the business deals with sensitive personal information or not.
3) Consent for Collection:[95] Rule 5 provides that before

---

92 Rule-3 of Information technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

93 Rule-4: Body Corporate to provide Policy for Privacy and Disclosure of Information.

94 Rule 5(9) of Information technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

95 Rule-5: Collection of information: Body corporate or any person on its behalf shall obtain consent in writing through letter or Fax or email from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information.

collecting sensitive personal information of individuals, the body corporate should obtain the prior consent of the provider of the information. The consent of the information provider can be obtained through any means including fax, letter or email. While asking for the consent, the body corporate should furnish the option to the information providers to provide or to not to provide such information.[96] Where the information provider opts for not providing the information, the body corporate is not liable to provide goods and services for which information is sought.

4) Notification:[97] The body corporate should follow the procedure to ensure that information provider is aware of the fact a) that his information is being collected, b) what is the purpose for which information is collected, c) that the purpose for which they are collected is lawful, d) who are the recipient of the information, e) name and address of the agency though which information is collected.
5) Consent for disclosure:[98] The Rule says that when the body corporate is disclosing the individuals' information to any third party, the body corporate is required to take the prior consent of information provider before disclosure. This prior consent is not required where the disclosure is made to government.
6) Use and Retention of Information:[99] The body corporate cannot retain the sensitive personal information for longer than that is required for the purposes for which information may be lawfully used or is otherwise required under any other law.
7) Right to access, correction and withdrawal:[100] The body corporate ensures that the information providers are having a right a review their collected sensitive personal information as well as a right to withdraw their consent in writing to the collection, use and transfer of information in future transactions. Body corporate should also ensure that whenever the information of the individuals is found inaccurate or deficient, will be duly rectified.

---

96 Rule 5(7) of Information technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
97 Rule 5(2) & 5(3) of Information technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
98 Rule 6: Disclosure of information.
99 Rule 5(4) of Information technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
100 Rule 5(7) of Information technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

8) Transfer of Information[101] (Transitional Transfer): A body corporate or any person who has collected the sensitive personal data or information on behalf of it may transfer such information to any other body corporate or person in India, or located in any other country, provided a) that the body corporate and person to whom the information is transferred has ensured the same level of protection as is provided under the Indian legal rules, b) that information is to be transferred only if such transfer is required for the performance of a lawful contract between the body corporate and the information provider, or c) that the information provider has given his consent to such transfer.
9) Reasonable Security Practices and Procedures:[102] The Information Technology (Amendment) Act, 2008 has provided an obligation on the body corporate to maintain and to implement the 'reasonable security practice and procedure'[103] for the protection of sensitive data protection or information of their consumers. To hold on these security procedures the Rules mention that security procedure would be either (a) the IS/ISO/IEC 27001 on Information Technology – Security Techniques – Information Security Management System – Requirements; or (b) a code developed by an industry association and approved and notified by the government. Rule 8(1) has mentioned that comprehensive documented information security program and security policies of body corporate should contain managerial, technical, operational and physical security control measures that are proportionate with the information assets being protected with the nature of business.[104]
10) Regular Audit of Security Procedures: Rule 8 (4) further provides that body corporate should engage an independent auditor (who is appointed by the Government India) to audit the security procedures on the regular basis. This Rule further provides that such audit should be carried out at least once a year or as and when the body

---

101 Rule-7: Transfer of information, Information technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

102 Rule-8: Reasonable Security Practices and Procedures, Information technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

103 Section 43A , Explanation (ii): Reasonable Security Practices and Procedures.

104 See Rule 8(1) of Information technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

corporate has undertaken a significant upgrading of its computer resource.

6. Critical Review of Data Protection Rules, 2011

1) Provisions of Data Protection Rules are primarily applicable to sensitive personal data or information and only a few provisions are related to personal information.[105] Adequate legal protection is required for all the personal information (Sensitive or Non-sensitive) disclosed in the electronic transactions because personal information includes the Personally Identifiable Information that can be used to exclusively identify, contact, or locate a single person or can be used with other sources to exclusively identify a single individual.[106]
2) Opt-in and opt-out clause should be interpreted with reference to the adequacy of security procedures opted by the company.
3) In the Rules, at some places references are given to sensitive personal information and at other places references are given to the personal information and to information in general. This creates an ambiguity whether such provisions apply to all information, personal information or only to sensitive personal data or information.
4) Rules provide that it is mandatory for the body corporate to take the written consent of the information provider for the use and transfer of sensitive personal information. Hence it rakes up an issue that if any personal information does not qualify for the category of 'sensitive personal information', such personal information can be used and

---

105 Rule-2(1)(i) of Data Protection Rules 2011 defined 'Personal Information' as any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person. (June 3, 2015), http://en.wikipedia.org/wiki/Personally_identifiable_information.

106 *See,* Australia, Information Privacy Principles under the Privacy Act 1988, Principle No. 4, (June 3, 2015), www.privacy.gov.au/publications/ipps.html; AICPA and the Canadian Institute of Chartered Accountants (CICA), Generally Accepted Privacy principles, Principle No. 8, (June 3, 2015), http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles; APEC, Privacy principles, Principle No. 7, (June 3, 2015), http://austlii.edu.au/~graham/APEC/APECv10.doc; US-EU Safe Harbor Privacy Principles, (June 3, 2015), www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm; Direct Marketing Association, Online Marketing Guidelines, (June 3, 2015), www.thedma.org/guidelines/onlineguidelines.shtml.

processed without the consent of the information provider under the terms of the contract.

5) Mode of Consent: The Data Protection Rules requires body corporate to take the consent of information provider in writing either by the means of letter, or fax or email. With the strict interpretation, it is assumed that consent cannot be acquired through standard form of electronic contract or by the way of acceptance of the privacy policy framed by body corporate. Such intricacy and detailed procedure of taking consent may affect the growth of businesses.
6) At some places, rules are made applicable to all information of information provider. In such cases the rules have broadened the scope and applicability of data protection rules. In such enlarged scope of data protection, it will be too intricate for the companies to maintain these data protection standards for all the information in general. Strict compliance of these standards may affect the growth of businesses.
7) The rules are applicable to the body corporate or any person located in India. Hence in association with IT (Amendment) Act, 2008, it can be assumed that if the body corporate or the person is located in India or is using any computer, computer network or computer resource located in India, then only the data protection rules will be applicable, but if the body corporate or person is neither located in India nor they are using any computer resource located in India, then data protection rules will not be applicable. Kamlesh Bajaj[107] asserted that foreign companies are not supposed to take consent of the consumers before collecting data of Indian consumers in their countries. Only the companies in India and the collection and transfer of data carried out in India are subject to Indian data protection regulation. Hence the data protection rules are limited in its extra-territorial application for the protection data privacy in electronic transactions.
8) Execution Period: Data protection rules have not provided any transition or execution period. The rules come into effect with an immediate effect. The Immediate effect has made a hurried application of rules by the body corporate.[108] In the hurried implementation, it is doubted

---

107 Bajaj Kamlesh, *Data Protection Standards Through Contracts*, RISE/C-PET: European Submit on Biometrics and Security in Global Perspective (2011).

108 Section 43A, Explanation (i): 'Body Corporate' means any company and includes a firm, sole proprietorship or other association of individuals engaged

whether privacy policies are effectively drafted or not.

9) It can be drawn that rules are basically enacted to facilitate the body corporate with a procedure to use individual's sensitive information (procedure that how, when and with which purpose the body corporate can use, process and transfer the sensitive personal information of individuals). They should speak more specifically on the obligation of the body corporate to protect the information privacy of the data subjects.
10) In Data Protection Rules, financial information is affixed generally with the sensitive personal information and the protection of financial information is not independently dealt with. As major part of the business information is financial in nature, high standard of privacy protection should be given to the financial information.[109] The inclusion of financial information with the information in general or sensitive personal information will require the body corporate to set high standard of privacy protection relating to all the information that is received in the ordinary course of business. This requirement of providing high standard to all the information in general is likely to have disrupting effect on the advancement of electronic business. In Europe, financial information are dealt in a separate category and are provided a different level of privacy protection from that to information in general.
11) European law contains numerous exceptions under which some information cannot be accessed and collected by the body corporate. Indian data protection rules hardly provide a full-proof framework against unrestricted access, collection and use of the individual's information without affording adequate exception to free access to information. The restricted access to some critical information may ensure enhanced data protection in electronic transactions.
12) Rule 5(7) of the Data Protection Rules, 2011 provides an obligation on the body corporate to afford the information provider an option to withdraw his consent for the access and collection of the information. According to many

---

in commercial or professional activities.

109 US Congress's Gramm-Leach-Bliley Act (GLB), also known as the Financial Services Modernization Act of 1999 has given a special mention to financial information and specifically provided a high standard to the privacy protection of the information privacy (June 4, 2015), http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf.

researchers[110] the right of the information provider to 'withdraw' his consent is green and unrealistic in the usual business practices. Disclosure, exchange and flow of information are an imperative requirement for the conduct of business[111] (both online and offline). Businesses cannot be conducted if the information is not disclosed, used, exchanged in business transactions by the parties involved in the transactions. In such a case if one party is being given an option to withdraw the information so provided, then the conduct and continuation of such business activity will be impossible at the end of business communities. Once the information is provided and used by the business with the consent of the information provider, the information provider should not be given a legal right to withdraw the information in the middle of a transaction. This may impede the growth of businesses. In the same rule it is also provided that after the withdrawal of information the body corporate is not under compulsion to provide goods and services. Hence the conjunction of right of provider to withdraw the information and the right of the body corporate to withdraw sale and to furnish the goods and services will ultimately affect the growth of electronic businesses in the information and communication technology enabled society.

13) Rule 8 of the Data Protection Rules, 2011 provides that in case where the provider and the recipient of information have not agreed on the standard of reasonable security practices for the protection of information privacy, then the body corporate may adopt the reasonable security practice either in the form of IS/ISO/IEC 27001 or in the form of reasonable security practice code developed by an industry association or body of such association and duly approved by the government. This provision has raised some important concerns: 1) in cases where the standard form of contracts are followed by the body corporate, where will come the point of the consent of the information provider in farming of security practices, 2) until now, government has not notified any duly approved security practices for the body corporate to follow in option, 3) as the

---

110 Nishith Desai and Associates, Working Paper on Technology Law Analysis, (2011) (June4,2015), http://www.nishithdesai.com/New_Hotline/IT/Technology%20Law%20Analysis_June1811.htm.

111 E-Commerce Growth Prospects Remain Strong, *Corporate EFT Report,* January 17, 2001.

IS/ISO/IEC 27001standards are globally accepted and internationally applicable, they can support the protection of information privacy and growth of e-commerce transactions at a global level. Under the predictable advantages of IS/ISO/IEC 27001, the recognition of these standards is made optional and not mandatory, 4) banks and the large business organizations should follow IS/ISO/IEC 27001 standard to boost the growth of business at global level, so the applicability of IS/ISO/IEC 27001 to the banking, large business organizations and alike organizations should be made mandatory.

14) Last but not the least the data protection rules are not applicable to the government and government organizations, which is the largest processor of personal and sensitive personal information in our country. The government websites are also likely to disclose information either consensually or in some hacking attacks etc., for example in December 2010, the CBI websites were hacked by the Pakistani hackers.[112] Hence the exemption to the government organization from data protection rules is putting individual's privacy right in danger.

In the light of the above discussion, it can be assumed that no doubt Indian legislature has attempted to provide data protection law for protecting information privacy, yet the legal provisions seems to be ambiguous to counteract the global challenges of privacy protection in the electronic transactions. The vagueness in the provisions of data protection rules like complicated application of sensitive personal data, personal data, requirement of written consent, concept of standard form of contract etc. are hindering the balanced application towards data protection with the growth of e-commerce. Thus, it is submitted that the present data protection statutory regime should be amended to remove the ambiguity in the present legal system for the protection of the information with balanced growth of e-commerce at global standards.

---

112 The Times of India, December 4th, 2010 (June 4, 2015), http://articles.timesofindia.indiatimes.com/2010-12-04/india/28249073_1_pakistani-cyber-army-pakistani-cyber-army-cbi-website.

7. Data Privacy Bill, 2011: Critical Analysis

The Press Information Bureau, Government of India, through their release[113] (Release ID: 74743) on August 18th, 2011 revealed that the Government is proposes to bring out a legislation for providing protection to individuals in case their privacy is breached through unlawful means. For this purpose, it is working on 'Right to Privacy' Bill. They further said that drafting of the legislation is at a very preliminary stage and details of the legislation are yet to be finalized. Accordingly, Ministry of Home Affairs, Government of India released the Working Draft Bill on Right to Privacy on September 29th, 2011.[114] The Privacy Bill, 2011 comes with an object of providing right to privacy to citizens of India and to regulate the collection, maintenance, use and dissemination of their personal information and to provide for penal action for violation of such rights and for matters connected therewith or incidental thereto.

Naavi Vijayashankar, in a discussion over Right to Privacy Bill 2011[115] identified the essential features of good privacy legislation as follows: a) providing an enforceable right to privacy, b) establishing an effective monitoring mechanism, c) imposing responsibilities on the data processor, d) defining and determining non-compliance deterrent structure, e) providing a grievance redressal mechanism, f) avoiding or minimizing overlapping of its provisions with other legislations. In the light of above principles, major provisions of the Bill[116] for the purpose of protecting right to privacy and its regulation are critically analyzed as follows:

1. Right to Privacy: Though the Bill creates a statutory Right to Privacy but under Section 3(1) right to privacy has been made subject to any law for the time being in force. It means that right to privacy under Privacy Bill in addition to existing laws on right toprivacy and not in their derogation. Therefore, any existing law which is in conflict

---

113 Ministry of Personnel, Public Grievances & Pensions, Right to Privacy Bill, 2011 (June 2nd, 2015), http://pib.nic.in/newsite/erelease.aspx?relid=74743.

114 *See* Draft Bill on Right to Privacy, 2011. No.II/20034/250/2011-IS-II, Government of India, Ministry of Home Affairs, IS-I Div (IS-II Desk) (June 2nd, 2013), http://www.naavi.org/cl_editorial_12/new_version_privacy_bill.pdf.

115 Vijayashankar Naavi, Analysis of the Right to 'Privacy Bill' 2011, Privacy Matters, Indian Institute of Technology, Bombay (2012) (May 14th, 2013), http://cis-india.org/internet-governance/proposed-privacy-bill.

116 *See* Gupta Apar, Analysis of Privacy Bill, 2011, Indian Law and Technology Blog (June 2nd, 2015), http://www.iltb.net/2011/06/analysis-of-the-privacy-bill-2011/.

with any of the directive and form of right to privacy under Section-3 will enjoy preference and legal validity[117] and may bypass the statutory right to privacy under Privacy Bill, 2011.

2. Definition of Right to Privacy: Various researchers[118] viewed that 'Right to Privacy' should ensure full protection to personal liberty in person and protection as against the unwarranted constraints by the society. They further opine that for adequate protection of privacy rights, right to privacy should include prospects of liberty, dignity and control.[119] Under this perspective, the definition of right to privacy under this Bill does not seem to be an extensive definition. It only provides that what will constitute as infringement of privacy and what will not constitute infringement of privacy.
3. Personally Identifiable Information & Non-Personally Identifiable Information: The Bill provides the broad definition of privacy[120], while defining what will constitute infringement of privacy and what will not be considered as infringement of privacy. The Bill has not defined right to privacy under the perspective of personally identifiable information and non-personally identifiable information. This classification seems to be vital for as it create an extent for the protection of personally identifying information and non-personally identifying information.[121] This classification further supports a balance in the protection of data privacy by e-commerce companies and their smooth growth at global platform.
4. Imprecision of exemptions: The Right to Privacy is not absolute in the Bill as it identifies various privacy breaches[122] permitted on the ground of sovereignty, integrity, security of India, prevention of public disorder, protection of rights and freedom of others etc. Some

---

117 *Ibid.*

118 Warren & Brandeis, *The Right to Privacy*, Harvard Law Review, Vol. 4, No. 5 (1890).

119 *See* Privacy and Civil Liberties Policy Development Guide and Implementation Templates, Global Justice Information Sharing Initiative, United States Department of Justice (May 23rd, 2015), http://www.search.org/files/pdf/Privacy_Guide_Final.pdf.

120 Chapter-II: Collection, Processing, Storage and Disclosure of Personal Data, The Right to Privacy Bill, 2011.

121 McCallister Erika *et al.*, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, National Institute of Standard and Technology, U.S. Department of Commerce (2010) (June 10th, 2015), http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

122 Exception to the Infringement of Privacy under Section 4, Privacy Bill, 2011.

exemptions like protection of freedom and rights of others seems to be vague as what rights and freedom will be under the jurisdiction of this Section and who will be the others; whether it will include all persons or only the citizens. Hence it requires clarity on this aspect. Apart from it, preventing the incitement to crimes also seems to be too vague and it can be misused.

5. Personal Information, Sensitive Personal Information & Essential Information: The Bill majorly applies to personal information, wherein few provisions like Section-12[123] deals with sensitive personal information. It is suggested that data should be divided into three categories: a) Personal Data,[124] b) Sensitive Personal Data[125] & c) Essential Data.[126] Data protection rules also should be classified accordingly. Level-I protection norms should be applicable to personal data, level-II protection norms (stricter) should be applicable to sensitive personal data and essential data should fall under the purview of permitted infringements. Essential Data by its definition means the data which requires mandatory disclosure to public in larger public interest and hence can be outside the privacy related control. Essential data majorly fall within the ambit of 'Right to Information' and 'Right to Freedom of Expression'.
6. Establishment of Regulatory Mechanism: The Bill suggested the establishment of Data Protection Authority[127] as an administrative body. It will exercise control and will supervise the compliance of data protection rules to the private parties involved in collection and storage of personal data. It addition to it Cyber Appellate Tribunal,[128] set up under Information Technology (Amendment) Act, 2008 is suggested as Dispute Redress Mechanism. Primarily the Bill seeks to create a division of power within these two bodies but in practice they seem to be in conflict with each other. For

---

123 Section-12: Processing of Sensitive Personal Data.

124 Personal Data is a data about the basic identity of the individuals.

125 Sensitive Personal Data refers a data which individual has absolute right to keep confidential like his private diary.

126 Essential Data refers a data which society has a right to know, like communicable disease carried by some person which has direct effect on the society.

127 Chapter-VI: Data Protection Authority of India, The Right to Privacy Bill, 2011.

128 Chapter-IX: Settlement of Disputes, The Right to Privacy Bill, 2011, Section-50: Appellate Tribunals.

example, Section 40(x)[129] of the Bill states that one of the functions of Data Protection Authority is to receive and to investigate complaints about alleged violations of data protection and to issue appropriate orders. This indicates that Data Protection Authority is vested with a sort with investigatory and adjudicatory powers. It seems that Bill does not make the grade to create a clear division of administrative and adjudicatory powers between Data Protection Authority and Cyber Appellate Tribunal.

7. Cyber Appellate Tribunal: The Bill indicated Cyber Appellate Tribunal constituted under Information Technology (Amendment) Act, 2008[130] for the settlement of disputes.[131] It is entrusted with the responsibility of court of first trial for some complaints[132] as well as court of appellate jurisdiction.[133] At present, there is only one office of Cyber Appellate Tribunal at Delhi which seems to be burdened with the matters under IT (Amendment) Act, 2008.[134] Therefore there is an urgent need either to provide for separate benches for the matters under Privacy Bill, 2011 or they should be limited to appellate jurisdiction for disputes under Privacy Bill, 2011.
8. Offences & Penalties: The Bill provides for elaborate structure of offences and Penalties[135] including civil remedies and criminal sanctions. It seems that several provisions are too complex and are in direct conflict with Information Technology (Amendment) Act, 2008 and Telegraph Act, 1885. For example, under Section 2(viii), consent includes implied consent wherein IT (Amendment) Act, 2008 requires written consent. Section 63 of the Bill provides courts cannot take cognizance of an offence except under a compliant made by authorities, wherein in IT (Amendment) Act, 2008, courts can take cognizance at the instance of aggrieved party as well.
9. Majority of electronic contracts are in the appearance of

---

129 Section 40(x): The Functions of Data Protection Authority shall be : to receive and investigate complaints about alleged violation of data protection in respect of the matters covered under Chapter-III and to issue appropriate orders and directions.

130 *See* Section-48: Establishment of Cyber Appellate Tribunal.

131 Chapter-IX: Settlement of Disputes, The Right to Privacy Bill, 2011, Section-50: Appellate Tribunals.

132 Section 50(1), The Privacy Bill, 2011.

133 Section 50(2), The Privacy Bill, 2011.

134 *See* Sachdeva Samir, Cyber Appellate Tribunal, National Seminar on Cyber Laws, New Delhi (2010)

135 Chapter-X: Offences & Penalties, The Right to Privacy Bill, 2011.

standard form of contract where terms are predetermined by companies and consumers have no option except to accept them for availing electronic services. This aspect of e-commerce and loss of data privacy in such transactions seems to be neglected under Privacy Bill, 2011.

Conclusion

The above discussion clarifies that although the government is vigilant in making timely changes in the law on data privacy, yet the present proposed bill does not seem adequate in protecting data privacy with a vision to ensure growth in e-commerce. Hence, it gives the impression that the Privacy Bill is suffering with some confusion, conflicts and overlapping for considering it as a comprehensive piece of privacy protection legislation. It requires some substantial review, clarity and additions towards enhanced and balanced protection of data privacy with inclusive growth of e-commerce.