Data Privacy Regulation: Recent Developments and Indian Response

Abhijit Rohi
Doctoral Research Candidate, National Law School of India University (NLSIU), Bangalore, Karnataka, India.

Abstract

The identification of models for privacy regulation is imperative in order to ascertain the nature of privacy model required in India. Justice A P Shah Committee, in its report has given a model to be adopted in India in the year 2012. The recommended model involved establishment of a privacy commissioner, nine national privacy principles, and a co-regulatory privacy framework for India - with industry defining best practices and the privacy commissioner approving and enforcing the same. The government of India has not adopted the given model or any other for privacy regulation in the country. Also since 2012 there have been some developments in the area of privacy regulation across the globe.

The paper deals with identification, in brief, of existing legal regime for privacy protection in India; outlines the recommendations of Justice A P Shah Committee for regulating Privacy; identifies the alternative models of regulation more specifically the ones adopted in the USA and the EU. With respect to the USA the focus is on the changes brought in by the US Judicial Redress Act, 2015. The EU model is studied on the basis of the comparison between EU Directive of 1995 for privacy protection and the EU Regulation of 2016, keeping in view the EU-U.S. Privacy Shield, it also aims at drawing specific lessons for India based on the analysis of the models adopted in the EU and the USA and their comparison with the model suggested in Justice A P Shah Committee Report.

KEYWORDS: Legal Regulations, Privacy, Regulation.

Introduction

Advent and proliferation of information technology has revolutionized the field of information generation, storage, processing and transfer. The byproduct of this revolution, one of the many, is threat to the individual privacy. The information has developed an intrinsic economic value and so followed the commercial exploitation of information concerning an individual. In the present 'data-driven economy' the companies make profits based on the personal data collected.[1]

The very nature of the technology is such that it captures every action and movement of an individual in an online environment making it privacy invasive. The recent developments in technology have opened up new avenues for information collection, storing and manipulation. The advent and quick expansion of fields of cloud computing and data analytics are testimony to this. As more and more data is being collected and used for increasing gains by the corporate and also by the governments, with or without consent or sometimes an ill-informed consent, it is important to look afresh at the legal regulation securing the privacy as well as other interests of an individual.

The concept of privacy is one of those legal concepts, the meaning and scope of which is still disputed and debated. The concept encompasses with itself various aspects of an individual's personality and life. Privacy can then be associated with the body of a person, being physical privacy, communication between individuals, being communicational privacy and information relating to an individual, being informational privacy. Informational privacy is the ability to determine for yourself when and how others may collect and use your information.[2]

The identification of models for privacy regulation is imperative in order to ascertain the nature of privacy model required in India. Justice A P Shah Committee, in its report has given a model to be adopted in India in the year 2012. The recommended model involved establishment of a privacy commissioner, nine national privacy principles, and a co-regulatory privacy framework for India - with industry defining best practices and the privacy commissioner approving and enforcing the same. The government of India has not adopted the given model or any other for privacy regulation in the country. Also since 2012 there have been some developments in the area of privacy regulation across the globe.

The paper deals with identification, in brief, of existing legal regime for privacy protection in India; outlines the recommendations of Justice A P Shah Committee for regulating Privacy; identifies the alternative models of regulation more specifically the ones adopted in the USA and the EU. With respect to the USA the focus is on the changes brought in by the US Judicial Redress Act, 2015. The EU model is studied on the basis of the comparison between EU Directive of 1995 for privacy protection and the EU Regulation of 2016. It also aims at drawing specific lessons for India based on the analysis of the models adopted in the EU and the USA and their comparison with the model suggested in Justice A P Shah Committee Report.

Privacy Protection in India: Current Regime

Before dealing with as to how India Regulates Privacy, a look into how India recognizes privacy is important. As pointed out, earlier in this paper, India recognizes the concept privacy indirectly.

A. Legislative Attempts:

Very few statutes make reference to the term 'privacy'. Two major enactments which refer to the term are firstly, Information Technology Act, 2000 (as Amended in 2008)[3] and secondly; The Right to Information Act, 2005.[4] The IT Act, 2000, under Sections 43A and 72 grants protection to the information collected about a person. The government of India has passed rules in furtherance of Section 43A.[5] These rules define both the expressions viz. 'personal information'[6] and 'sensitive personal data or information'[7] under Rule 2. On the other hand the concept of privacy as envisaged under Section 66E is primarily relating to the physical or bodily privacy of a person. Thus primarily only legal provisions protecting informational privacy in India are Section 43A, 72 of the IT Act, 2000 and Section 8(1)(j) of the RTI Act, 2005 along with the Sensitive Personal Information Rules, 2011. This indicates the inadequate legislative attention received by the concept of privacy in India.

The preceding part indicates that the Indian legal regime had not prioritized protection of privacy, with the introduction of Aadhaar Scheme major questions are being raised aiming at protection of privacy. Also to note that the IT Act, 2000 did very little to protect privacy of citizens in an online environment till the insertion of Section 43A in 2008 and the Sensitive Personal Information Rules in 2011. These attempts are not

flawless and are being criticized for being inadequate. This part deals with critically analyzing these attempts from a global perspective.

The Sensitive Personal Information Rules, 2011 are applicable only to 'body corporate,'[8] the definition of which does not include the data collected by government bodies and individuals. Thus there is no recourse against the government for collection, storage, manipulation, disclosure or transfer of data.

The Sensitive Personal Information Rules, 2011 are criticized by the privacy advocates on various grounds namely, the Sensitive Personal Information Rules poorly define 'body corporate,' state entities involved in collection of personal and sensitive personal information is precluded from the its scope. Emphasizing the importance of the prior consent of the individual providing personal and sensitive personal information, as the case may be, the Rule 5(1)[9] mandates the consent to be taken by the body corporate only when it is collecting sensitive personal data, implying that no consent is requited in collection of personal data, this Rule also does not mention in detail the nature of consent. Though the need of the consent regime has been clearly established,[10] it has also been criticized on very pertinent issues, such as cognitive problems in making informed rational choices, structural problems as too many institutions collecting information, privacy self-management fails to address larger social values to state a few.[11]Rule 5(2)[12] highlighting lawful purpose, nexus between the function and data collected, and necessity of the data for the said purpose and Rule 5(4)[13] concerning the retention of data collected also applies only to sensitive personal information and leaves personal information completely out of their scope.

Rule 6(1)[14] also applies only to sensitive personal data instead of all personal information. The use of the phrase "*any third party*" lends vagueness to this provision since the term "third party" has not been defined. The phrase "*provider of information*" is undefined and creates confusion as it could mean either or both of the individual who consents to the collection of his personal information or another entity that transfers personal information to the body corporate. The Sensitive Personal Information Rules, 2011 suffer from numerous flaws, incapacitating the effective protection of privacy of an individual.

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 is passed in order to secure the data collected both demographic and biometric information in order to issue Unique Identification Number to every individual. The preamble of the legislation states 'An Act to provide for, as a good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services, the expenditure for which is incurred from the Consolidated Fund of India, to individuals residing in India through assigning of unique identity numbers to such individuals and for matters connected therewith or incidental thereto.' The concern for privacy or data protection is not reflected as a priority in the preamble.

B. Judicial Perspective:

Briefly describing the judicial attention gained by the concept of privacy, it is imperative to make reference to some of the most prominent judicial pronouncements in India. Firstly, *Kharak Singh v. State of Uttar Pradesh*,[15] in a minority judgment in this case, Subba Rao J. held that "the right to personal liberty takes in not only a right to be free from restrictions placed on his movements, but also free from

encroachments on his private life. It is true our Constitution does not expressly declare a right to privacy as a fundamental right but the said right is an essential ingredient of personal liberty. Every democratic country sanctifies domestic life; it is expected to give him rest, physical happiness, peace of mind and security. In the last resort, a person's house, where he lives with his family, is his "castle" "it is his rampart against encroachment on his personal liberty." This case, especially the observations by Subba Rao J., paved the way for later elaborations on the right to privacy using Article 21 in India.

Secondly, *Govind v. State of Madhya Pradesh*, [16] concerning privacy, more specifically with surveillance by domiciliary visits, the Court stated, "too broad a definition of privacy will raise serious questions about the propriety of judicial reliance on a right that is not explicit in the Constitution. The right to privacy will, therefore, necessarily, have to go through a process of case by case development. Hence, assuming that the right to personal liberty, the right to move freely throughout India and the freedom of speech create an independent fundamental right of privacy as an emanation from them it could not be absolute. It must be subject to restriction on the basis of compelling public interest." Thus for the first time the highest Court in India has declared right to privacy as a fundamental right warning clearly against the absolute nature of the same.

Thirdly, *R. Rajagopal v. State of Tamil Nadu*,[17] in which the court was involved in balancing of the right of privacy of citizens against the right of the press to criticize and comment on acts and conduct of public officials. The right of privacy of citizens was dealt with by the Supreme Court in the following terms: - "(1) The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a 'right to be let alone'. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, childbearing and education among other matters. None can publish anything concerning the above matters without his consent - whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages. Position may, however, be different, if a person voluntarily thrusts himself into controversy or voluntarily invites or raises a controversy. (2) The rule aforesaid is subject to the exception, that any publication concerning the aforesaid aspects becomes unobjectionable if such publication is based upon public records including court records. This is for the reason that once a matter becomes a matter of public record, the right to privacy no longer subsists and it becomes a legitimate subject for comment by press and media among others. We are, however, of the opinion that in the interests of decency [Article 19(2)] an exception must be carved out to this rule, viz., a female who is the victim of a sexual assault, kidnap, abduction or a like offence should not further be subjected to the indignity of her name and the incident being publicised in press/media." Thus this judgment was also the reiteration of *Govind's Case*[18], the important fact highlighted pertaining to the nature of privacy was calling it 'a right to be let alone'.

Fourthly, *People's Union for Civil Liberties v. Union of India*,[19] it was a public interest litigation, in which the court was called upon to consider whether wiretapping was an unconstitutional infringement of a citizen's right to privacy. On the concept of the 'right to privacy' in India, the Court made the following observations: "The right privacy - by itself - has not been identified under the Constitution. As a concept it may be too broad and moralistic to define it judicially. Whether right to privacy can be claimed or has been infringed in a given case would depend on the facts of the said

case." This judgment had an effect of having enforceable right to privacy but not having a determined scope of it and leaving to be decided subjectively.

Fifthly, *Mr. 'X' v. Hospital 'Z'*,[20] this case involved a claim for damages made by a patient against a hospital which disclosed the fact that the patient tested positive for HIV which resulted in his proposed marriage being called off and the patient being ostracized by the community. The case revolved around balancing right to privacy if Mr. X, the appellant with that of right to life of Ms. Y, with whom the marriage of the appellant was settled. The Court said that the disclosure of the information by Hospital Z did not amount to violation right to privacy of the appellant.

And lastly, *State of Maharashtra v. Bharat Shanti Lal Shah*,[21] wherein the court reiterated the position in all previous judgments and also stated "The interception of conversation though constitutes an invasion of an individual right to privacy but the said right can be curtailed in accordance to procedure validly established by law. Thus what the Court is required to see is that the procedure itself must be fair, just and reasonable and non arbitrary, fanciful or oppressive."

It is imperative to note that among all these cases, only one, that is, *Mr. 'X' v. Hospital 'Z'*[22] dealt with disclosing or divulging the information concerning an individual. Other cases dealt primarily with interception of the communication between the parties by the state, thus implying the violation of 'communication privacy.' Interesting to note also that there have been numerous instances of reference to specific rights enshrined under Article 19 of the Constitution of India viz. in *Kharak Singh's Case*, [23] *Govind's Case*, [24] Article 19(1)(d) and Article 19(5) guaranteeing to a citizen a right to privacy of movements, in *R. Rajagopal's Case*,[25] dealing with freedom of press vis-à-vis right to privacy, Article 19(1)(a) and Article 19(2). The references to freedoms under Article 19 and corresponding restrictions under the same imply the existence of unbreakable link between the freedoms under Article 19 and personal liberty as enshrined under Article 21.

R. Rajagopal's Case[26] and *Mr. 'X' v. Hospital 'Z'*[27] stand differently from rest other cases as stated before on certain grounds. The major point of differentiation being the nature of privacy claimed in both these cases. As opposed to the other cases, the protection sought by the affected parties does not relate to the violation of privacy of their communication, it also does not deal with violation of their physical privacy; rather these cases seek protection of information concerning the parties alleging the violation of right to privacy. These cases, thus illustrate the different aspect of privacy which needed protection in their cases, viz. privacy of the information or 'informational privacy'.

Even though this has been the judicial view towards privacy over the years, currently, whether there exists a fundamental right to privacy under the Constitution of India is being questioned before the Supreme Court of India. A petition filed by Justice K.S. Puttaswamy (Retd.) challenging the constitutional validity of Aadhaar Scheme is being heard by the Court. In his arguments representing the Government of India, Attorney-General, stated that privacy is not a fundamental right.[28] The Court referred the matter to the Constitutional Bench consisting of 9 judges to authoritatively decide the constitutional matter relating to right to privacy.[29] On August 24, 2017 the Supreme Court has decided that the decision in M P Sharma[30] and Kharak Singh which holds right to privacy is not protected by the Constitution stands over-ruled and also that Right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III

of the Constitution.[31] The Court in this case for the first time has made reference to the concept of data protection. The matter about the constitutional validity of Aadhaar Scheme is yet to be decided.

Thus looking at the existing regime in India it is clear that there is limited attention received by the concept of privacy by legislature and the judiciary. The right to privacy is recognized by the judiciary in the instant petition then owing to Article 32 of the Constitution of India any citizen can knock the doors of the Supreme Court to get right to privacy enforced. But according to Article 12 this right to get right to privacy enforced will accrue only against the authorities which fall within the meaning of 'state'; thus not guaranteeing protection against privacy invasive actions of the private entities.

Owing to the absence of the clear, more precise construction of right to privacy, its legislative recognition with corresponding legal regulation is imperative. Keeping this in view, the 'Group of Experts on Privacy' was constituted by the Planning Commission under the Chairmanship of Justice A P Shah which has submitted its Report on October 16, 2012.

Recommendations of Justice A P Shah Committee Report:[32]

In the recent past the Report of the Expert Committee headed by Justice A. P. Shah assumes a special importance to highlight the inadequate treatment received by the concept of privacy in India. The Report 'has identified a set of recommendations, which government may like to consider while formulating the proposed framework for a Privacy Act.' The Report clearly states that –

> 'Information is beginning to be collected on a regular basis through statutory requirements and through e-governance projects. This information ranges from data related to: health, travel, taxes, religion, education, financial status, employment, disability, living situation, welfare status, citizenship status, marriage status, crime record etc. At the moment there is no overarching policy speaking to the collection of information by the government. This has led to ambiguity over who is allowed to collect data, what data can be collected, what are the rights of the individual, and how the right to privacy will be protected. The extent of personal information being held by various service providers, and especially the enhanced potential for convergence that digitization carries with it is a matter that raises issues about privacy.'

With respect to the changed nature of technology and its advancement in the recent years the Report makes a clear mention of the fact that –

> '[…] on the Internet, multiple data flows take place simultaneously, *via* phenomena such as web 2.0, online social networking, search engine, and cloud computing. This has led to ubiquity of data transfers over the Internet, and enhanced economic importance of data processing… While this is exposing individuals to more privacy risks, it is also challenging businesses which are collecting the data directly entered by users, or through their actions without their knowledge, […] and correlating the same through more advanced analytic tools to generate economic value out of data.'

As privacy as a concept, at times, may be considered as subjective, the privacy protection and its extent may depend upon the nature of the society, its culture and inadvertently the value attached to, by them, to privacy. The Report looks at the initiatives by different jurisdictions emphasizing the commonality of privacy protection principles followed in all those jurisdictions, it indicates the possibility of all agreeing to 'Universal Privacy Protection Principles.' The Report compares the data protection principles in the Organization for Economic Co-operation and Development (OECD) Privacy Guidelines, EU Data Protection Directives, Asia-Pacific Economic Cooperation (APEC) Privacy Framework, Canada PIPEDA (Personal Information Protection and Electronic Documents Act), and Australia ANPP (Australia National Privacy Principles). It then identifies nine principles viz. notice, choice and consent, collection limitation, purpose limitation, access and correction, disclosure of information, security, openness and accountability, together called 'National Privacy Principles' to be adopted in India.

The Report proposes the Privacy Act for India recognizing multidimensional privacy, horizontal applicability, conformity with privacy principles and co-regulatory enforcement regime. The Committee has also recommended the establishment of privacy commissioners at the Central and Regional levels, a Privacy Act bringing in a system of co-regulation that will give self-regulatory organizations (SROs) at the industry level the choice to develop privacy standards, mandatory appointments of data controllers and privacy officers.[33]

Thus the model proposed in the Report

The Government of India is yet to act on the recommendations of the Committee highlighting the inadequacies in the privacy protection standards and legal regime in India. Ever since the publication of the Report there have been a lot of developments at the international level and many countries have made changes in the existing privacy regulations. The following parts deal with recent enactments in the USA and the EU.

Privacy Regulation Model Adopted in the USA:

Right to privacy is recognized as personal and fundamental right protected under the Constitution of the United States.[34] In order to provide certain safeguards for an individual against an invasion of personal privacy by the collection, maintenance, use, and dissemination of personal information by Federal agencies the US Congress has enacted the Privacy Act of 1974.[35] The Privacy Act protects individuals against the Federal Agencies handling personal information.

The USA has adopted self-regulation approach for data protection for the data handled by the private parties and companies. Federal Trade Commission (FTC), primarily aiming at the protection of the interest of the consumers and focusing on the fairness in data collection has released Fair Information Practices Principles in 2000[36] which have been criticized for its limited scope and for being non-enforceable. Also these principles are considered inadequate as compared to eight privacy protection principles issued by the Privacy Office of the Department of Homeland Security in 2008 which are closely aligned with the OECD principles.[37]

Very recently, the Obama administration intended to pass the Consumer Privacy Bill of Rights Act, the draft of which was released by the White House once again in 2015.[38] The Draft appears to be hinting to the adoption of international standards for privacy protection and also an attempt to have an umbrella data protection law for the

USA. The White House in February 2012 issued 'Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy', [39] which advocated the idea for having Consumer Privacy Bill of Rights Act.

The USA has passed the Judicial Redress Act, 2015, with a primary intention to extend Privacy Act remedies to citizens of certified states.[40] It provides for the 'civil remedies' for 'intentional or willful disclosure' of a 'covered record' of a 'covered person' from a 'covered country'.[41]

The privacy protection regulation model in the USA is much scattered as there are various legislations dealing with various regulatory aspects of privacy protection. There are legislations at the federal and at state level too. The laws are made according to sectoral approach. This is evident form presence of numerous legislations and absence of one umbrella legislation for data protection. The Federal Trade Commission Act[42] as a federal consumer protection law, the Children's Online privacy Protection Act (COPPA) [43] which applies to the online collection of information from the children, the Financial Services Modernization Act (Gramm-Leach-Bliley Act (GLB))[44] for regulation collection, use and disclosure of financial information, the Health Insurance Portability and Accountability act (HIPPA)[45] for regulation of medical information, the controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) [46] along with the Telephone Consumer Protection Act[47] to respectively regulate the collection and use of e-mail addresses and telephone numbers, the Electronic Communications Privacy Act[48] and the Computer Fraud Abuse Act [49] for regulating the interception of electronic communications and computer tampering respectively, etc. are some prominent examples of the federal legislations regulation information collection use and disclosure for the specific sectors. Other than these there are many laws at the state level. 'Most states have enacted some privacy legislation, however California leads the way in privacy arena, having enacted laws like the Shine the Light law[50] which requires companies to disclose details of the third parties with whom they have shared their information and also the data security law[51] which requires the businesses to implement and maintain reasonable security procedures to protect personal information from unauthorized access, destruction, use, modification or disclosure.'[52] These recent developments in California take it closer to the EU model of privacy protection.

As per the recommendations in the Report the rights-based model bases right to privacy at its center unlike the USA model which is termed as the one with 'obscure vision.' [53] The USA regulates privacy more importantly protects individual's informational privacy primarily from the perspective of consumer protection. The regulating authority in the USA is Federal Trade Commission (FTC) as opposed to Data Protection Commissioners in the UK. Thus the USA model for privacy protection is characterized by self-regulation approach, sectoral approach and is criticized for obscurity, non-recognition of various principles such as data minimization, mandatory destruction of data, etc., and non-enforceability of various fair information practice principles.

Privacy Regulation Model Adopted in the European Union:

The EU Regime is characterized by presence of a Directive[54] and has been modified very recently by the adoption of the General Data Protection Regulation (GDPR)[55] in 2016. In January 2012, the European Commission proposed a comprehensive reform

of data protection rules in the EU.[56] On May 4, 2016, the official texts of the Regulation and the Directive have been published in the EU Official Journal in all the official languages. While the GDPR entered into force on May 24, 2016, it shall apply from May 25, 2018.[57]

The GDPR 'protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data,'[58] thus it specifically recognizes the right to the protection of personal data. The Regulation also lists out the principles relating to processing of personal data.[59] The Principles are lawfulness, fairness and transparency in processing of data; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality and accountability. The GDPR defines and highlights the difference between 'personal data' and 'special categories of personal data'; it also defines genetic data, biometric data and data concerning health. The GDPR, under Chapter IV, lays down the obligations and responsibilities of controllers and processors. Chapter III of GDPR lists out numerous rights of the data subject and a corresponding duty is created in favor of the controller to comply. The rights are as follows:

Right to information[60]

Right to lodge a complaint with supervisory authority[61]

Right of access by the data subject[62]

Right to rectification[63]

Right to erasure (right to be forgotten)[64]

Right to restriction of processing[65]

Right to data portability[66]

Right to object[67]

Right not to be subject to a decision based solely on automated processing, including profiling[68]

Right to an effective judicial remedy against a supervisory authority[69]

Right to an effective judicial remedy against a controller or processor[70]

Right to compensation and liability[71]

For the purposes of giving effect to these rights the GDPR introduces few technical concepts in the legal arena which are profiling,[72] pseudonymisation,[73] data protection by design.[74] The GDPR stresses the employment of data protection impact assessment (DPIA) 'where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons'[75] and consultation with 'the supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.'[76]

The GDPR also provides for drawing up code of conduct for various provisions of the Regulation,[77] establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with the Regulation,[78] and the transfer of personal data to third countries and international organizations.[79] The Regulation mandates for the establishment by 'each Member State of one or more independent public authorities, called supervisory authorities,

which are to be responsible for monitoring the application of the Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union.'[80] The Regulation establishes the' European Data Protection Board' where each Member State is represented through representative of respective supervisory authorities.[81]

Lessons for India:

The recommendations in the Report appear to move Indian privacy protection regime closer to the approach adopted in the UK and the EU. A model which is rights based one and where there is single legislation addressing all the issues concerning information protection, like the Data Protection Act, 1998 of the UK and General Data Protection Regulation (GDPR)[82]of the EU. But there are some important issues to be addressed by India. They are as follows:

1. The proposed legislation is proposed to be titled as the Privacy Act; the drafters have to be cautious about the use of the term 'privacy' as there are many unresolved jurisprudential issues about the meaning of the term and its scope. Also rather than calling it Right to privacy in cyberspace it is important to use the expression used by the EU, that is, to call it 'right to the protection of personal data'.
2. Having umbrella legislation for the purposes of data protection can be considered to be a welcome move which resembles to the approach in the EU and the USA (particularly the Obama Administration) seems to be planning to adopt the similar position though from the point of view of protection of consumers' interest.
3. The recognition distinctly of all the stake holders is absolutely important. Thus definitions of data subjects, data controllers, data processors etc. are to be clearly laid down. Also the government and any department of the government has also to be bound by the provision so of such a legislation.
4. Rights based approach appears to be best suited to the Indian needs. So the law should clearly mention the right of data subjects as against all other stake holders. Right to erasure (right to be forgotten) and also right to data portability be a legal right available.
5. Data protection principles are to be exhaustively recognized and their implementation be modified according to the needs of Indian data subjects.
6. Conducting Privacy Impact Assessments (PIAs) of any new technology being used or which is about to be introduced in the market must be made mandatory for all the controllers and processors.
7. The proposed law must deal with certain technical concepts as data mining, individual data profiling and also big data analytics etc. The law is expected to set the legal ground for adoption of new approach to privacy protection in cyberspace. The legal recognition and implementation of the concept of privacy by design (PBD) can be a pragmatic way in dealing with this issue. Also the application of pseudonymisation techniques while processing of personal data so as to avoid data mining and individual data profiling also needs to be legally implemented.
8. India shall have to devise a way of ensuring the timely up gradation of the law to suit the requirements of new technologies being invented and which are made publically available for their use. Thus the combination of legislative regulation and sector specific industrial self-regulation should be embodied in the law.

9. Also since most of the service providers who collect, store or even process data beyond the territories of India, the law has to cater to the issues arising out of such Transborder Data Flow (TDF).

Since the report of Justice A P Shah Committee in 2012, the international scenario has changed to a larger extent, with the adoption of the GDPR in the EU, Judicial Redress Act in the USA and materialization of the Privacy Shield Agreement between the EU and the USA. The Indian regime for privacy protection in the cyberspace has to be revamped drastically in order to secure right to privacy of its own citizens.

Conclusion

Thus far, the attempts on the part of legislature to recognize the right to privacy and as an offshoot of the same the right to data protection have been unsatisfying. The judiciary has recognized right to privacy as a fundamental right now. The development of data protection and its treatment as a right is still in a nascent stage in India which is detrimental to the interest of individuals, economy and the country. Conceptualizing right to data protection has to be soundly based in the nature of data and data controller, the use of data, objective of collection of data, extent of the control exercised by data subject on the data and a thorough causal and consequential analysis of data collection, storage, use, manipulation and transfer.

References

[1] Who owns your personal data? The incorporated woman, available at www.economist.com/blogs/schumpeter/2014/06/who-owns-your-personal-data (accessed on November 30, 2015).

[2] Robert H. Sloan and Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. HIGH TECH. L. 370 (2014).

[3] Hereinafter referred to as IT Act, 2000.

Section 43A: Compensation for failure to protect data: *Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected.*

Explanation: For the purposes of this section

(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities

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

(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

Section 66E: Punishment for violation of privacy: *Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person*

without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both

Explanation.- For the purposes of this section—

(a) —transmit means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) —capture, with respect to an image, means to videotape, photograph, film or record by any means;

(c) —private area means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

(d) —publishes means reproduction in the printed or electronic form and making it available for public;

(e) —under circumstances violating privacy means circumstances in which a person can have a reasonable expectation that—

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

Section 72: 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 thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.*

[4] Hereinafter referred to as the RTI Act, 2005.

Section 8: Exemption from disclosure of information: *(1) Notwithstanding anything contained in this Act, there shall be no obligation to give any citizen, - …(j) information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information.*

[5] The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. Hereinafter referred to as Sensitive Personal Information Rules, 2011.

[6] Rule 2(1)(i): *"Personal information" means 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.*

[7] Rule 3: *"Sensitive personal data or information" of a person means such personal information which consists of information 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:
provided that, any information that is freely available or accessible in public domain or furnished under the 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 purposes of these rules.

[8] As defined under Section 43A of IT ACT, 2000.

[9]Rule 5 - Collection of Information - (1) *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.*

[10]Robert H. Sloan and Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. HIGH TECH. L. 370 (2014). 'Adequate informational privacy requires a sufficiently broad ability to give or withhold free and informed consent to proposed uses.'

[11]*See*Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126, HARV. L. REV. 1880 (2013). It has also been contended that the privacy violation happens as 'a result of an aggregation of pieces of data over a period of time by different entities.'

[12]Rule 5(2) - *Body corporate or any person on its behalf shall not collect sensitive personal data or information unless —*
(a) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and
(b) the collection of the sensitive personal data or information is considered necessary for that purpose.

[13]Rule 5(4) - *Body corporate or any person on its behalf holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.*

[14]Rule 6(1) - *Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation:*
Provided that the information shall be shared, without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. The Government agency shall send a request in writing to the body corporate possessing the sensitive personal data or information stating clearly the purpose of seeking such information. The Government agency shall also state that the information so obtained shall not be published or shared with any other person.

[15] A.I.R. 1963 S.C. 1295

[16] (1975) 2 S.C.C. 148.
[17] A.I.R. 1995 S.C. 264.
[18] (1975) 2 S.C.C. 148.
[19] (1997) 1 S.C.C. 301.
[20] (1998) 8 S.C.C. 296 (India) & (2003) 1 S.C.C. 500.
[21] (2008) 13 S.C.C. 5.
[22] (1998) 8 S.C.C. 296 (India) & (2003) 1 S.C.C. 500.
[23] A.I.R. 1963 S.C. 1295
[24] (1975) 2 S.C.C. 148
[25] A.I.R. 1995 S.C. 264
[26] A.I.R. 1995 S.C. 264
[27] (1998) 8 S.C.C. 296 (India) & (2003) 1 S.C.C. 500
[28] Krishnadas Rajgopal, *After 60 Years SC to Relook Right to Privacy, Courtesy Aadhaar*, (Last Acessed on October 9, 2015) (available at http://www.thehindu.com/news/national/after-60-years-sc-to-relook-right-to-privacy-courtesy-aadhaar/article7739356.ece)
[29] Krishnadas Rajgopal, *After 60 Years SC to Relook Right to Privacy, Courtesy Aadhaar*, (Last Acessed on October 9, 2015) (available at http://www.thehindu.com/news/national/after-60-years-sc-to-relook-right-to-privacy-courtesy-aadhaar/article7739356.ece).
[30] 1954 SCR 1077
[31] Justice K.S. Puttaswamy v. Union of India, the reportable version of the judgement is available at http://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf (Last Acessed on September 9, 2017)
[32] Report of the Group of Experts on Privacy, (Chaired by Justice A P Shah, Former Chief Justice, Delhi High Court), (Oct. 16, 2012) available at http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf (Accessed on November 30, 2012) (Hereinafter referred to as the Report).
[33] *Id.*
[34] Section 2 (a)(4) of 5 USC 552a.
[35] Title 5 U.S.C. § 522a.
[36] The Archived web page of FTC listing 'Fair Information Practice Principles' (Last Accessed on August 9, 2016) (available at https://web.archive.org/web/20090205180646/http://ftc.gov:80/reports/privacy3/fairinfo.shtm).
[37] Department of Homeland Security, Privacy Policy Guidance Memorandum (2008) (Memorandum Number 2008-1), https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf
[38] Administration Discussion Draft (Last Accessed on October 9, 2015) (available at https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf).
[39] A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (Last Accessed on October 9, 2015) (available at https://www.whitehouse.gov/sites/default/files/privacy-final.pdf).
[40] As stated in the preamble of the Judicial Redress Act, 2015. The Act was enacted by 114th Congress of the USA at the Second Session held on January 4, 2016.
[41] Section 2 of the Judicial Redress Act, 2015.
[42] 15U.S.C. §§41-58.

[43] 15 U.S.C. §§6501-6506.
[44] 15 U.S.C. §§6801-6827.
[45] 42 U.S.C. §1301.
[46] 15 U.S.C. §§7701-7713 and 18 U.S.C. §1037.
[47] 47 U.S.C. §227.
[48] 18 U.S.C. §2510.
[49] 18 U.S.C. §1030.
[50] Cal. Civil Code. §§1798.83-1798.84.
[51] Cal. Civil Code. §1798.81.5.
[52]Ieuan Jolly, Loeb & Loeb LLP, *Data Protection in United States: Overview*, (Last Accessed on October 9, 2015) (available at http://uk.practicallaw.com/6-502-0467#).
[53]*See* Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 Emory L.J. 911 (1996).
[54]Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[55]Regulation (EU) 2016/679, Regulation on the Protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC.
[56]EUROPEAN COMMISSION - PRESS RELEASE, Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses (Last Accessed on October 22, 2015) (Available at http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en).
[57] Protection of Personal Data, (Last Accessed on August 22, 2016) (Available at http://ec.europa.eu/justice/data-protection/).
[58] Article 1 of GDPR.
[59] Article 5 of GDPR.
[60] Articles 13 and 14 of GDPR.
[61] Id., Article 77 of GDPR.
[62] Article 15 of GDPR.
[63] Article 16 of GDPR.
[64] Article 17 of GDPR.
[65] Article 18 of GDPR.
[66] Article 20 of GDPR.
[67] Article 21 of GDPR.
[68] Article 22 of GDPR.
[69] Article 78 of GDPR.
[70] Article 79 of GDPR.
[71] Article 82 of GDPR.
[72] Article 4(4) of GDPR.
[73] Article 4(5) of GDPR.
[7474] Article 25 of GDPR.
[75] Article 35 of GDPR.
[76] Article 36 of GDPR.
[77] Article 40 of GDPR.
[78] Article 42 of GDPR.
[79] Chapter V of GDPR.
[80] Chapter VI of GDPR.
[81] Article 68 of GDPR.
[82] Regulation (EU) 2016/679.