NLSIU/WP2019

Working Paper Series

2019

Paper Four

PRIVACY AND DATA PROTECTION LAWS IN INDIA

National Law School of India University

Table of Contents

About the Author and Reviewer

Ms. Pavithra R.

Assistant Professor of Law, Christ [Deemed-to-be University] and a Doctoral Scholar at the National Law School of India University.

Ms. Architha Narayanan

B.A LL.B, Masters in Public Policy & Assistant Professor of Law, NLSIU.

Executive Summary

Internet communication and technology has provided new way of doing business. It has enhanced the scope of business innovation. New changes have facilitated interaction among the Government, business entities, stakeholders and consumers. Changes in the business transaction and communication led to collection of huge sets of data. With data-sets being created, issues of trust, misuse, abuse and online cybercrime activities came into limelight. These concerns have raised debates and concerns over privacy and security of information. These events in turn led to considering individual privacy in their personal life and their informational privacy in internet medium heart of legislation requiring privacy and data protection. Global economy is tilted in favour of connecting information and data around the corners of the world. Repeated attempts of transfer of data are taken to ensure that international trade and commerce are proliferated to the required level. This brings in the complexities of cross-border flow of data that not only affects the individuals, but also the business networks and governments. Harnessing the potential of information and communication and technology is become a mandate with changing dynamics in business-consumer relationship and with cross-border business connection. There is need to find a balance between the issues regarding privacy and informational privacy between the stakeholders at hand. Data has become a commercial asset whose value has become multi-fold than what it was two decades back. It has become directly associated with the digital economy. In the earlier times, violation of data rights and privacy of the individual were considered as a tort and a tortious liability was attached to those infringed upon data rights. There were certain international interpretations, conventions and principles that propounded as to how data could be utilized and further process took place on that basis. Relating to protecting of individual privacy and informational privacy, there exists no stand-alone

international treaty or a model convention that could be relied upon by the Countries to propose a new law in the given area. However, the global market and economic impact that the data carries today, it has become inevitable to create a new legislative environment. At present, the privacy and data protection regime are governed by the Indian Information Technology Act, 2000. Sec.43A of the Act is the core provision that provides for protection of personal data by the body corporate. The Act has uncertainties and misfits that require changes in the present context. The regulatory situation at present in the nation is far from the ideal policy framework as necessitated by the Sustainable Development Goals. To this end, came the Justice Puttaswamy case declaring right to privacy, a fundamental right under Article 21 of Constitution of India. To strengthen the right further, Srikrishna Committee Report paved way for legislation by rolling out the Personal Data Protection Bill, 2018. In the given background, the policy paper is divided into five major parts. Part I focuses on privacy being an in-definitive term and tries to review the definition of privacy. Part II seeks to analyse the 'Privacy Puttaswamy Case' and 'Aadhar Puttaswamy Case' to understand the nuances of declared fundamental right and the kind of data protection regime that is required in India. It also seeks to identify and analyse the key concerns in the Personal Data Protection Bill, 2018 along with the comprehensive analysis of Srikrishna Committee Report and has sought to fill in the lacunas in the committee report in its Part III. Part IV details of the possibility of contextualizing General Data Protection Regulation (GDPR) of European Union in Indian regime. Last part provides for the recommendations/key takeaways of the policy paper that could be considered in bringing about a comprehensive legislation towards protecting privacy including informational privacy of the individual.

1. Introduction and Background Information

At the outset, privacy and data protection provide for a sense of autonomy over personal information of individual over the societal intervention. With technological advancements and political state, the public space in the state has widened. The expanded public space shrunk the private space through state surveillance, law and order. The intervention is in specific aimed at protecting the interests of the public space. In addition, collective actions of community disturbed privacy of the individual. The term privacy is a reference term used from time immemorial to ascertain individual autonomy over personal and bodily affairs.

Control over personal information extends not only to physical existence but also to decisions and ideas of the existence. It is essential to ensure that autonomy of individual personal and bodily space is not interfered with. It is mutually important to respect the distinction between private and personal life. These commonalities demand for a boarder understanding of privacy, its perspectives, constituents, facets, domains, rules, and regulations that is in effect. Protecting privacy in India has been achieved through varied legislative attempts including the tort law, medical laws, family laws, financial laws etc. With passage of time, the scattered legislation could not address the growing intrusion by state and general society. Hence, there were serious questions of law posed before the judiciary. Constant judicial intervention upheld the rights of individual protecting their personal space, information and decisions. Numerous judicial decisions considered privacy as an implied fundamental right that could not be violated without due process of law.

Recently, privacy has been declared as a fundamental right in India through judicial pronouncement. It has been declared integral right to an individual in several other jurisdictions. With the growth of information and technology, development of commerce in electronic medium, privacy came to be understood in varied facets. Privacy has become an

umbrella concept to accommodate clusters of concept within its ambit. It inter alia includes individual privacy, communication privacy, informational privacy, decisional privacy, location privacy etc. Data is nothing but the information of an individual processed in the digital medium. Data accumulated for decades have become data sets and big data.

While privacy is individual centric and involves disturbance in any form, information of the individual collected in the due course amounted to considerable amount of data in the hands of the collector. Data as a concept came with accumulation of information for specific set of purposes and assimilation in a prescribed manner. It has resulted in mapping of an individual behaviour through processing using computer and internet. Gradually, it formed the core of data analytics, big data and an asset with unforeseen commercial value. Assimilation of information gave rise to the otherwise called informational privacy. It proscribes collection of individual data for unwarranted purposes and prescribes for protection of data from unauthorized access. The constant intrusion in the informational privacy has triggered the debates of formulating policies of data protection.

Current times demand the need to protect data not only against entities and business groups but also from the hands of the government. There is a growing need to protect privacy and data from misuse, unauthorized intrusion and regulation of all sought of relationship, be it with state or non-state entities. From the foetus to the deceased, from animals to birds, from living to non-living, from corporations to collective, existence and privacy has become co-relational. If all the information is considered private, all intrusion would become violation of privacy. Therefore, there is a need to ensure that violation of sensitive information relating to an individual is construed as against the norms and laws.

The techniques to obtain information, to process it as data increased the demand-supply flow of data of individual without their consent. Not being regulated has resulted in usage of

individual data as a key asset in large scale business. The formation of cloud has changed the location base of the data. With cloud and growing multinational businesses, protecting data of individual and also unlocking free flow of data has acquired a transnational perspective. The borderless nature of data requires data protection regime to ensure that data of the nationals that are processed by a foreign entity/ website to be given adequate protection within and cross-border territory.

Informational privacy has its origins from the legal right to privacy. Interpretation of privacy has resulted in it becoming a more general and basic fundamental right guaranteed to the individual. Computer complexities has made informational privacy a specialized field of privacy right and has validated the need for own set of rules and regulations. Though general protection rights are derivates of fundamental right to privacy, they have been fine-tuned to accommodate the special purposes of protecting data. Hence, laws relating to informational privacy in order to sustain growing information technology have become detailed and technical aspect that stands separate from the general privacy laws.

Countries around the world has recognized the importance of data in growth of their economy and are actively involved in law making process for privacy and data protection. Understanding privacy and informational privacy as specific rights, Indian Courts and Committees have dealt with their differences in an admirable fashion. India deliberated on the angels of privacy being a fundamental right in the 2017 Puttaswamy case. This historical judgment paved way for Ministry of Electronics and Information Technology to pronounce a need for the law in the area. The Ministry formed a Justice B N Srikrishna Committee with a humongous task of preparing a report to deliberate on need for protecting privacy and informational privacy. The report with the expert member group was released in 2018. Based on the report came a bill called the Personal Data Protection Bill, 2018. The main intent of

the bill is to bring in a data protection framework by prescribing the ways in the organisations are duty bound to operate, purpose of collecting data, storage, offences, penalties and jurisdiction of the Courts to decide disputes.

In light of the judgment, committee report and the Bill, there have been effective steps taken to bring about an effective and efficient legal framework to govern privacy and data protection in India. It is with the given background that the Policy Paper thrives to analyse

- Efficacy of steps taken to regulate privacy and informational privacy (data protection) in India.
- Need to balance them against other legitimate and legal considerations.
- Address the gaps in the existing laws and to accommodate the gaps with possible suggestions.
- Importance of contextualising General Data Protection Regulation of European Union in India.
- Consider other issues that may be deemed appropriate in changing technological times.

2. Legal Framework to Privacy: Law and Judicial Insight

Not being observed and not being disturbed are fundamental and integral part to life and living of a being. Every individual deserve to be in a state where they feel free and away from the eyes of strangers and observation of public. They have a right to private life which stresses upon solidarity. Solidarity as an aspect becomes essential in order to loosen individual inhibitions, to promote self-awareness, self-direction, for human oneness and uniqueness and for them to be saved from oppression of the commonness.

Directly connected with the levels of anonymity, the notion of privacy gives strength to the individual to be secured and secluded without any intrusion and interference into their affairs. Security and seclusion would in essence be attained only when individuals and community of being, feel more confident about their information and that there is due care, caution and consideration given in order to protect the same. It ensures the space that is necessitated is provided for each individual without any unauthorized intrusion.

Privacy begins with individual. It is attained when the individual has complete right to control what effectively happens with their information. Ultimately, a right to have in their possession and custody, certain facts of their lives, their individual preferences, choices etc. The right is determined and intertwined with the ability of the individual to control the outsiders from having knowledge and information about one self. The form and notion of privacy in varied instances overlaps with other concepts inter-alia secrecy, confidentiality, solidarity, liberty, protection and guaranteed freedoms from unwanted intrusion.

Factually, privacy holds a position similar to maintaining a ‘zero-relationship’ with another person or group or the society. It signifies the importance of absence of interaction, communication and perception among the family, peer, work and society. It would hold well against a single individual or from the pluralistic society as a whole. The wings of privacy are

extraordinary and have grown multi-fold to include issues correlated to thought, sentiments and emotional attachments.

In earlier times and small circles, though every other person knew the deepest of information about one another, life was such that sensitive areas and issues were not subjected to debate in public. However, in modern times, due to active intersection of private lives with the public spaces and for a, negotiating individual privacy in the world of social contract has become increasingly difficult. It has created a conundrum that has become difficult to solve in a period of time with changing civility and cohesion.

While being stressed upon to protect the private and personal interest of an individual from the public, a relevant question of who and what exactly forms a relevant part of private on one side and public on the other. Understanding the private-public divide and demarcating the same would help simplify the complexities that privacy has attained recently. The distinction between the public and private though in the outset looks simple; it is multifaceted and multifarious without any clear distinction in terms of perspectives and relationships.

Comprehension of precise legal boundaries of where exactly the public action, intrusion and interference has to end and from where exactly the private space begins have to be ascertained to maintain a zero-relationship status and to demarcate a private-public gap. Developing a substantive public-private divide has eventually become difficult and has been left to be determined on a case to case basis. This position has led to further debate of the actual nature of privacy and hence, series of cases landed in judicial forums to clarify privacy in a given instance along with tasks to the adjudication bodies to decide whether in a particular scenario, public had intruded into the space of private and broke the zero-relationship status.

Though achieving privacy in essence has become dependent on facts and circumstances in numerous instances, it continues to provide entitlements to individuals. One of the assertions

is protection of individual autonomy and their private space over the spheres of their public space. It asserts that private presupposes the public and would continue to do so as a reasonable expectation to the test of privacy.

2.1 Definition of Privacy

Privacy revolves around the concept of individual autonomy. However, protecting one's autonomy has become a major concern with changing times and conditions. To address the concern, reaching out to the core part of what constitutes privacy and framing a definition, or much less, an operational definition is essential. Identifying its meets and bounds, evaluating its essence, scope and limitation without giving too broad or too narrow a definition is a mammoth task in itself. Varied judges through their obiter have expressed the concerns surrounding the definition of privacy. Apprehensions have time and again been raised claiming that defining privacy would raise questions of propriety of judiciary.

Privacy, an abstract term that is combined with cumulative factors does not find a stand-alone definition in any legislation within or outside the territories of the nation. The term finds its first definition as early as 1890, in a famous article written by two judges named Samuel Warren and Louis Brandeis. While addressing the impact of growing technology on privacy of individuals, the authors defined privacy as 'the right to be left alone'. It guarantees an individual to have in his custody certain facts, choices and preferences to himself and not necessary to reveal the same to outside world. Therefore, it could be asserted that privacy allows self-possession of certain facts to the individual alone. This ideology has been incorporated and also forms the base of recently formulated General Data Protection Laws of European Union.

The judge gave definition could not address varied number of problems that surrounded the abstract notion of privacy. Since it did not survive the leaps of technological advancement, Logan Roots while authoring a short article to a magazine defined privacy as 'the freedom to

selectively reveal one's self'. A remarkable shift from the judge's definition to the magazine definition is that judges, Samuel and Louis claim privacy as a right whereas Roots claim privacy as freedom attributed to the individual. This gave rise to the classic debate over whether privacy should be considered as a right or as freedom or as privilege.

Decades later, Prof. Winster held that the definition as pronounced by the judges and Roots do not fit in with several technological leap. Specific issues were raised in terms of increased societal scrutiny in individual spaces and state surveillance as a means that claimed to protect societal interests and for security purposes. These issues became a focal point of argument in his article tilted Privacy and Freedom. Professor in his writings advocated privacy to be broader than being left alone and of individual's right to selectively reveal information. He defined privacy as a claim belonging to individuals, groups or institutions. Privacy was an ordained right where the individuals, groups or institutions would have an absolute control to determine when, how and what extent of information about them would be communicated to others. Therefore, privacy came to be held in terms of discretion coupled with right and freedom.

W A Parent in his writing 'A New Definition of Privacy for the Law' ascribed privacy in terms of documentation and having cognitive access to the same. He claims that information, if any, about an individual documented would not come under the purview of privacy. He claims privacy as that condition where undocumented personal information about an individual is kept outside others knowledge. Though control based view was retained as an integral component, there was a shift that required individuals to identify whether information is disclosed or not.

Twentieth century witnesses a combination of technological development, increased social media space and also constant state surveillance claiming safety and security. With growth in technology, individuals tend to give away information that they are in absolute control of.

Further, with state intrusion becoming norm of the day, identifying what information could be eyed on and what should not be, were left unidentified. Therefore, drafting an all-in-one encompassing definition that accommodates all the ingredients of the right has become difficult.

In recent times, both legislature and the courts have taken proactive steps to recognize right to privacy as fundamental rights in different jurisdictions. However, there exists no exhaustive definition or conception of what exactly would constitute privacy. One common demonstration is that it has been construed as an umbrella term containing a cluster of rights and paving way for numerous rights originating from privacy as a parent right.

2.2 Privacy and Aadhar Puttaswamy Case Analysis: Justice K.S Puttaswamy (Retd.) v. Union of India[1]

The nine-judge bench of the Supreme Court unanimously recognized that the Constitution guaranteed the right to privacy as an intrinsic part of the right to life and personal liberty under Article 21. The landmark judgment that was delivered on the 24th of August 2017 held that the absence of an express constitutional guarantee of privacy does not necessarily warrant that there is no protection of privacy under the framework of protected rights including those in Article 19 and 21. The Supreme Court has overruled the case of *M.P. Sharma v. Satish Chandra*[2] which was rendered by a bench of 8 Judges and *Kharak Singh* v *State of UP*[3] which was rendered by a bench of 6 judges wherein it was observed that the Constitution does not expressly protect the Right to Privacy.

[1] 2017 (10) SCALE 1
[2] 1954 AIR 300
[3] 1963 AIR 1295

2.2.1 Interpretation of the Term 'Privacy' by the Bench

On a plain reading of the judgment it can be observed that the *right to privacy* was reinforced by the concurring opinions of the judges. The judges recognized that this right includes autonomy over personal decisions (For e.g. consumption of beef), bodily integrity (e.g. reproductive rights) as well as the protection of personal information (e.g. privacy of health records). The concurring judgments had also included some specific implications of this right. The interpretations are mentioned below-

Justice Chandrachud (on behalf of himself, C.J. Kehar, J. Agrawal and J. Nazeer) in his opinion stated that privacy was not surrendered entirely when an individual is in the public sphere. To elaborate further he added the analysis of how the right to privacy is essentially a negative right against State interference, as in the case of criminalization of homosexuality, as well as the positive right to be protected by the State[4].

It can be inferred from his opinion that life and personal liberty are not merely creations of the Constitution but are rights that are recognised by the Constitution as inhering in each individual as an intrinsic and inseparable part of the human element which dwells within. This is a highly appreciated opinion as not only is the right recognized in the constitution but the importance of its origin is highlighted. While privacy is termed as a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution an importance is also given to the various elements of privacy that arise from various contexts and facets of freedom and dignity which are recognised and guaranteed by the fundamental rights contained in Part III[5];

It is important to note that Justice Chandrachud holds Privacy as the constitutional core of human dignity. He entails that privacy has both a normative and descriptive function. He

[4] Para 122, K.S Puttaswamy v. Union of India 2017 (10) SCALE 1
[5] Para 10 K.S Puttaswamy v.Union of India 2017 10 SCALE 1.

differentiates it further and classifies that in normative level privacy sub-serves those eternal values upon which the guarantees of life, liberty and freedom are founded. At a descriptive level, privacy postulates a bundle of entitlements and interests which lie at the foundation of ordered liberty. Privacy includes at its core the preservation of *personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation.*

Privacy also connotes a right to be left alone. Privacy safeguards individual autonomy and recognises the ability of the individual to control vital aspects of his or her life. Personal choices governing a way of life are intrinsic to privacy. Privacy protects heterogeneity and recognises the plurality and diversity of our culture. While the legitimate expectation of privacy may vary from the intimate zone to the private zone and from the private to the public arenas, it is important to understand that privacy is not lost or surrendered merely because the individual is in a public place. Privacy attaches to the person since it is an essential facet of the dignity of the human being; Justice Chandrachud holds the importance of why the Constitution must evolve with the necessities of time to meet the challenges thrown up in a democratic order governed by the Rule of law. He states that the meaning of the Constitution cannot be frozen on the perspectives present when it was adopted and agrees to the fact that technological change has given rise to concerns which were not present seven decades ago and the rapid growth of technology may render obsolescent many notions of the present.

Thus, interpretation of the Constitution must be resilient and flexible to allow future generations to adapt its content bearing in mind its basic or essential features, while saying so, lays down the examples of when other rights which form part of the fundamental freedom protected by Part III, including the right to life and personal liberty It is agreed upon that Under Article 21, privacy is not an absolute right. A law which encroaches upon privacy will have to withstand the touchstone of permissible restrictions on fundamental rights. In the

context of Article 21 an invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable. Quoting from the judgement, it can be noted that the law must also be valid with reference to the encroachment on life and personal liberty Under Article 21.

An invasion of life or personal liberty must meet the three-fold requirement of

(i) legality, which postulates the existence of law;

(ii) need, defined in terms of a legitimate state aim; and

(iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them.

Justice Chandrachud also lays down that privacy has both positive and negative content. The negative content restrains the state from committing an intrusion upon the life and personal liberty of a citizen. Its positive content imposes an obligation on the state to take all necessary measures to protect the privacy of the individual. Decisions rendered by this Court subsequent to *Kharak Singh* v. *State*[6] upholding the right to privacy would be read subject to the above principles.[7]Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. The Justices commend to the Union Government the need to examine and put into place a robust regime for data protection.

The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state. The legitimate aims of the state would include for instance protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits. They agree upon that these are matters of policy to be considered by the Union

[6] (1964) 1 SCR332
[7] Para 107, K.S Puttaswamy v.Union of India 2017 10 SCALE 1.

government while designing a carefully structured regime for the protection of the data. They also note that the Union government has informed the Court that it has constituted a Committee chaired by Hon'ble Shri Justice B.N. Srikrishna, former Judge of this Court, for that purpose, the matter shall be dealt with appropriately by the Union government having due regard to what has been set out in this judgment.

A plain reading into *Justice Chelameswar's* opinion one can infer that within the context of right to privacy he had included a right to refuse medical treatment, a right against forced feeding, the right to consume beef and the right to display symbols of religion in one's personal appearance etc[8]. This opinion rendered by Justice Chalameswar brings in a variety of rights under the purview of right to privacy itself. Everyday habits including aesthetic, hygiene, medical and culinary choices, are included within the right to privacy. This interpretation of privacy is essential as it not only dignifies an individual's choices but also protects the same from unlawful interference from the State. The options canvassed for limiting the right to privacy include an Article 14 type reasonableness.

2.2.2 No Legal Right is Absolute

Justice Chelameshwar acknowledges the fact that no legal right can be absolute in nature and that every right has limitations. Therefore he admits that even a fundamental right to privacy has limitations and that the limitations were to be identified on case to case basis depending upon the nature of the privacy interest claimed. There were different standards of review to test infractions of fundamental rights. While the concept of reasonableness overarches Part III, it operates differently across Articles. While interpreting the Constitution's liberty guarantee to contain a fundamental right of privacy, it is held necessary to outline the manner

[8] Para 38, K.S Puttaswamy v.Union of India 2017 10 SCALE 1.

in which such a right to privacy could be limited. The just, fair and reasonable standard of review under Article 21 needs no further explanation or elaboration.

It has also most commonly been used in cases dealing with a privacy claim are made. *Gobind v. State of Madhya Pradesh*[9] resorted to the compelling state interest standard in addition to the Article 21 reasonableness enquiry. Only in privacy claims which deserve the strictest scrutiny was the standard of compelling State interest to be used. As for others, the just, fair and reasonable standard under Article 21 would apply. When the compelling State interest standard was to be employed must depend upon the context of concrete cases[10]. Thus, Justice Chelameswar concludes that the principle of 'every right has limitations' should apply to the concept of right to privacy laid down in Article 21 of the Indian Constitution.

Justice Bobde observed that the right to privacy can be determined when consent is obtained for the essential for distribution of inherently personal data such as health records. This interpretation concurs with the view of Justice Chalameswar as it highlights the importance of consent while individual personal data is distributed. Every individual is entitled to perform his actions in private. In other words, every individual is entitled to be in a state of repose and to work without being disturbed or even spied upon. Justice Bobde states that the entitlement to such a condition is not confined only to intimate spaces such as the bedroom or the washroom but even in a public place. He claims that privacy has a deep affinity with seclusion as well as such ideas as repose11.

Justice Bobde holds importance to how an individual looks at his or her own solitude, confidentiality and secrecy (in our communications) and intimacy. He also enumerates that solitude is always essential to privacy. It is in this sense of an individual's liberty to do things

[9] (1975) 2 SCC 148
[10] Para 236, Justice K.S Puttaswany v. Union of India 2017 (10) SCALE 1
[11] Para 281 K.S Puttaswany v. Union of India 2017 (10) SCALE 1

privately that a group of individuals, however large, is entitled to seclude itself from others and be private. He even regards the importance of a conglomeration of individuals in a space to which the rights of admission are reserved - as in a hotel or a cinema hall -must be regarded as private. The law requires a specific authorization for search of a person even where there is suspicion. Privacy must also mean the effective guarantee of a zone of internal freedom in which to think. It is important to be able to keep one's work without publishing it in a condition which may be described as private. The vigour and vitality of the various expressive freedoms guaranteed by the Constitution depends on the existence of a corresponding guarantee of cognitive freedom.

2.2.3 Privacy and its Connection to Dignity and Liberty

Justice Bobde holds that Privacy, as an essential right is held to be essential and important in all contexts and societies, this however is not a descriptive right but is a normative one. The normative case for privacy is simplified - Nature has clothed man, amongst other things, with dignity and liberty so that he may be free to do what he will consistent with the freedom of another and to develop his faculties to the fullest measure necessary to live in happiness and peace. The Constitution, through its Part III, enumerates many of these freedoms and their corresponding rights as fundamental rights and privacy is an essential condition for the exercise of most of these freedoms.

Every right which is integral to the constitutional rights to dignity, life, personal liberty and freedom, as indeed the right to privacy is, must itself be regarded as a fundamental right. This was embodied in the judgement where the conclusion must be that an inalienable constitutional right to privacy is inherent in Part III of the Constitution. *M.P. Sharma* and the majority opinion in *Kharak Singh* must stand overruled to the extent that they indicate to the contrary. The right to privacy is inextricably bound up with all exercises of human liberty -

both as it is specifically enumerated across Part III, and as it is guaranteed in the residue Under Article 21. This right is distributed across the various articles in Part III and henceforth takes the form of whichever of their enjoyment its violation curtails. Any interference with privacy by an entity covered by Article 12's description of the 'state' must satisfy the tests applicable to whichever one or more of the Part III freedoms the interference affects[12]. Thus Justice Bobde holds the view that the concept of 'dignity' and 'liberty' is protected under the right to privacy.[13]

It can be inferred from reading *Justice Nariman's* concurring opinion that he has classified the facets of privacy into non-interference with the individual body, protection of personal information and autonomy over personal choices.[14] Justice Nariman holds that this right is subject to reasonable regulations made by the State to protect legitimate State interests or public interest. However, when it comes to restrictions on this right, the drill of various Articles to which the right relates must be followed. For example, if the restraint on privacy was over fundamental personal choices that an individual was to make, State action could be restrained under Article 21 read with Article 14 if it was arbitrary and unreasonable; and under Article 21 read with Article 19(1) (a) only if it relates to the subjects mentioned in Article 19(2) and the tests laid down by present Court for such legislation or subordinate legislation pass muster under the said Article.

Each of the tests evolved by this Court, via legislation or executive action, under Article 21 read with Article 14; or Article 21 read with Article 19(1)(a) in the aforesaid examples must be met in order that State action must hold up to. In the ultimate analysis, the balancing act that is to be carried out between individual, societal and State interests must be left to the training and expertise of the judicial mind. This reference is answered by stating that the

[12] Para 281 K.S Puttaswamy v. Union of India 2017 10 SCALE 1.
[13] Para 283 K.S Puttaswamy v. Union of India 2017 10 SCALE 1.
[14] Para 369 K.S Puttaswamy v. Union of India 2017 10 SCALE 1.

inalienable fundamental right to privacy resides in Article 21 and other fundamental freedoms contained in Part III of the Constitution of India.

Justice Sapre stated that in addition to its existence as an independent right, the right to privacy included an individual's rights to freedom of expression and movement and was essential to satisfy the constitutional aims of liberty and fraternity which ensured the dignity of the individual[15]. The right to privacy emanating from the two expressions of the preamble namely, 'liberty of thought, expression, belief, faith and worship' and 'fraternity assuring the dignity of the individual' and also emanating from Article 19(1)(a) which gives to every citizen a freedom of speech and expression and further emanating from Article 19(1)(d) which gives to every citizen 'a right to move freely throughout the territory of India' and lastly, emanating from the expression 'personal liberty' under Article 21.

Thus, the right to privacy is inbuilt in these expressions and flows from each of them and in juxtaposition. Right to privacy is a part of fundamental right of a citizen guaranteed under Part III of the Constitution. However, he too agrees that it is not an absolute right but is subject to certain reasonable restrictions, which the State is entitled to impose on the basis of social, moral and compelling public interest in accordance with law.

Justice Kaul stated that the Judge discussed the right to privacy with respect to protection of informational privacy and the right to preserve personal reputation. He said that the law must provide for data protection and regulate national security exceptions that allow for interception of data by the State. The Court also recognized that the right was not absolute but allowed for restriction where this was provided by law, corresponded to a legitimate aim of the State and was proportionate to the objective it sought to achieve. The right of privacy is a fundamental right. It is a right which protects the inner sphere of the individual from

[15] Para 69, K.S Puttaswamy v. Union of India 2017 10 SCALE 1.

interference from both State, and non-State actors and allows the individuals to make autonomous life choices.

If the individual permits someone to enter the house it does not mean that others could enter the house. The only check and balance is that it should not harm the other individual or affect his or her rights. This applies both to the physical form and to technology. He agrees to the fact that in an era where there are wide, varied social and cultural norms and more so in a country like ours which prides itself on its diversity, privacy is one of the most important rights to be protected both against State and non-State actors and be recognized as a fundamental right. He notes that it works out in its inter-play with other fundamental rights and when such restrictions would become necessary would depend on the factual matrix of each case. Thus, the fact that it may give rise to more litigation could hardly be the reason not to recognize this important, natural, primordial right as a fundamental right. He further concludes the necessity to let the right of privacy, an inherent right, be unequivocally a fundamental right embedded in part-III of the Constitution of India, but subject to the restrictions specified, relatable to that part.[16]

The judgment also rejected the submission that privacy is a privilege for the few. *"It is privacy which is a powerful guarantee if the state were to introduce compulsory drug trials of non-consenting men or women. The sanctity of marriage, the liberty of procreation, the choice of a family life and the dignity of being are matters which concern every individual irrespective of social strata or economic well-being. The pursuit of happiness is founded upon autonomy and dignity. Both are essential attributes of privacy which makes no distinction between the birth marks of individuals."*

2.2.4 State and Non- State Entities

[16] Para 496 K.S Puttaswamy v. Union of India 2017 10 SCALE 1.

It is essential to note that an important question was raised in the present judgment relating to the extent of enforceability of the right to privacy against non-state entities. A number of observations in the course of the Judgment are aimed at the applicability of the right to privacy to non-state actors. One to begin with is that, the court recognized that the right of privacy is a fundamental right. It determined that a right which protects the inner sphere of the individual from interference from both State and non-State actors and allows the individuals to make autonomous life choices.

The judgement recognised the claims of privacy against the State and non-State actors. In respect of the State, the judgement identified concerns of surveillance and profiling, whereas in respect of non-State actors, it emphasized on the impact of technology, in the form of pervasive data generation, collection, and use in a digital economy. Justice Kaul elaborated on the influence of big data, in particular, its impact on the actions of an individual and the resultant chilling effect it may have on free speech and expression. Justice Kaul emphasised the need to protect certain information from both the State as well as private actors.

Meanwhile, Justice Chandrachud acknowledged the importance of the right to privacy in the context of the age of "big data" i.e. data sets capable of being searched and marked by their exhaustive scope and permanency of collection. Justice Chandrachud elaborated on this within the context of *'Informational Privacy'* in the course of the Judgment. In specific, though, with regard to non-state entities, Justice Chandrachud makes certain important references non-state entities/actors. Justice Chandrachud noted that "The challenges which big data poses to privacy interests emanate from State and non-State entities" He also added *that "The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well."*

Justice Sanjay Kishan Kaul also observed that the capacity of non-state actors to invade privacy has been enhanced. He included the participation of non-state entities in the collection of data of individuals, citing examples of Uber, Facebook, Twitter and Airbnb to explain how personal information such a location, thoughts and preferences of individuals collected by non-state entities. He notes that this makes all individuals exposed to vulnerability of possible exploitation of such collected personal information. He states- *"Knowledge about a person gives a power over that person. The personal data collected is capable of effecting representations, influencing decision making processes and shaping behaviour. It can be used as a tool to exercise control over us like the 'big brother' State exercised. This can have a stultifying effect on the expression of dissent and difference of opinion, which no democracy can afford."*

The judgement overall stressed on the importance of unprecedented need for regulation regarding the extent to which such information can be stored, processed and used by non-state actors. It was stated that privacy is a limit on the government's power as well as the power of private sector entities. Justice Kaul's observations regarding private entities take on relevance as he recognised the right of an individual to deal with his personal data in a manner that he deems fit. *"...from the right to privacy in this modern age emanate certain other rights such as the right of individuals to exclusively commercially exploit their identity and personal information, to control the information that is available about them on the 'world wide web' and to disseminate certain personal information for limited purposes alone."* This observation has far reaching implications on various state as well as non-state actors who collect online information from individuals. The judgement recognised the right of every individual to be able to exercise control over his/her own life and image as portrayed to the world and to control commercial use of his/her identity, thereby possibly laying down ground for a ***'right to be let alone'*** similar to that provided for by the European Union. It is

further stated that- *"The right of privacy is a fundamental right. It is a right which protects the inner sphere of the individual from interference from both State, and non-State actors and allows the individuals to make autonomous life choices."*

While understanding the difference between the State Actors and the Non State Actors and how they infer the right to privacy, it is important to note that the new AADHAAR Judgement[17] wherein the AADHAR Act was held to be valid should be considered while determining how much of our right can be controlled by the State. In every right, the concept of proportionality is used to determine the legal standard for testing infringements of rights. Thus, it is important to note that the constitutional challenge to the Aadhaar programme and to the provisions of the Aadhaar Act mounted primarily on the touchstone of proportionality.

While one can note that the previous held this standard of proportionality to be vague which brought upon multiple hearings on this issue, the majority judgment attempts to provide some clarity on this point. It refers to the different shades of proportionality employed in different jurisdictions and had then adopted a different sense of the same. The requirement begins with something as simple as how there must exist a law (with adequate procedural safeguards), proportionality requires the following four requirements: a legitimate State aim, a rational nexus between the impugned measures and the aim and then that the impugned measure be the least restrictive method of achieving the aim and lastly that there must be a balance between the extent to which rights are infringed, and the overall public benefit.

On Surveillance, the majority decided to uphold the AADHAR programme on the ground that there is no such thing as constitutionally significant surveillance and upholds surveillance. However it is important to note that the Majority in this judgement avoid legal question by making a factual finding that the AADHAR project is incapable of being turned

[17] Citation to be added

into a surveillance engine. The Majority then also discusses that AADHAAR programme is compatible with principles of data protection.

On reading Justice Chandrachud's dissent[18] in the very same judgement, one can note that there is a difference in the legal standards and also a difference in how the AADHAAR programme works. .To give an example, on the issue of Whether Section 59 of the Aadhaar Act validates past action, the Majority and Justice Chandrachud disagree on the uniqueness of biometrics, or on the existence of exclusion. The question is not whether the Majority is right or if Justice Chandrachud is wrong, the question is whether who can afford to have the issue to be wrong in matters that concern with the right to privacy in the AADHAR era.

In Matters concerning Privacy, Justice Chandrachud dissent has a sound legal character. While the Majority undertakes the proportionality test by diminishing our privacy interest in our bodily characteristics, and devaluing the importance of biometric details (fingerprints or iris scans). Justice Chandrachud holds that it our privacy interests in our biometric details is high: both from an informational self-determination point of view, as well as from a bodily integrity and physical safety point of view. Justice Chandrachud is careful about two important issues, one on "minimal information (collected)" and second on "minimal interference with privacy".

While the Majority uses the fact that biometric details are given frequently and for a multiplicity of purposes, to argue that we don't have a heightened privacy interest in them Justice Chandrachud holds that what is relevant is that a "carefully designed" biometric system may nonetheless preserve privacy and that therefore that is the standard we must measure Aadhaar against. It is an important legal understanding that he finds that the absence of consent within the Act, the extent of information disclosed, the expansive scope of the

[18] Citation to be added

term “biometrics”, the burden placed upon the individual to update his/her own biometrics, and lack of access to the record, cumulatively constitute a serious infringement of privacy.

Justice Chandrachud’s dissenting judgment recognizes what the Aadhaar case was truly about why the Court is called upon to answer the relationship between technology, individual, State and Indian Constitution. The Aadhaar case was all about the relationship between the individual and the State, and how technology was altering and even potentially inverting that relationship. It was about how power worked itself through technology, through algorithms, becoming the arbiter of peoples’ rights and entitlements, while determining the position of the Constitution among all this. While the Majority celebrated the need for efficiency and unique identification, ignores the legal question involved. Justice Chandrachud discusses how unique data sets can lead to *“perpetuating of pre-existing inequalities”*. In retrospect, it is important to note that he refuses to use civil rights and socio-economic rights against one another and refuses to acknowledge how biometric systems are tried out with only welfare recipients. And it comes across most vividly in a brief discussion about identification and identity, an issue that controlled the hearings throughout.

3. Sri Krishna Committee Report – A Comprehensive Analysis

3.1 About the Report

India is at its rapid phase of growth using the avenues available in the digital environment. The growth has resulted in yield of digital economy. Digital landscape and economy revolve around information of the parties involved in the process. The information gets stored, processed, accessed to become data sets. To reap benefits in the digital world, it is important to ensure that information or data in the digital format is secure and has been dealt with proper caution. Understanding the importance of securing data, the Government of India constituted a ten-member Committee to formulate a report titled ‘A Free and Fair Digital

Economy- Protecting Privacy and Empowering Indians'.[19] The Committee of experts under the Chairmanship of Justice BN Srikrishna mainly pondered into the issues of privacy and data protection in India.[20] Upon analysis the issues, it came up with specific principles and recommendations divided into nine chapters. In essence, the report provides for a broad framework of data protection law. It addresses the way to encapsulate the framework and promulgate the same in India. The Report was also accompanied with a Data Protection Bill, 2018[21] that requires assent of the Parliament to form a first ever codified legislation to govern Privacy and Data Protection in India. Given the background, the Policy Paper proposes to chapter-wise analyse the contents of the Report and the Bill and provide areas that require reconsideration before it is passed as a governing legislation.

3.2 Chapter 1- A Free and Fair Digital Economy

India, at present, does not have a comprehensive legislation to deal with data protection and privacy. Hence, the chapter looked into the methodology adopted to protect with data in other jurisdictions inter alia United States (US), European Union (EU) and China. US follow a laissez-faire approach, a liberal approach to protect data. It provides for privacy as a right through its Constitutional framework and varied scattered legislations[22]. However, the jurisdiction does not possess single data protection law. No legislative efforts seem to be in place to consolidate the existing and scattered legislations.

EU on the other hand follows a strict legal regime and has enacted the General Data Protection Regulation, 2018 (GDPR)[23]. The Regulation treats information as power that has the potential of becoming a core component of business, commerce and international trade. It provides for a detailed legal framework of rights, duties and obligations of parties involved in

[19] http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf Srikrishna Committee Report accessed from.
[20] Office Memorandum MEITY dated 31 July 2017
[21] Link of the Bill
[22] Few Acts include Privacy Act, Privacy Act, 1974, Electronic Communications Privacy Act, 1986, Right to Financial Privacy Act, 1978, HIPPA
[23] Many nations follow GDPR to bring data protection legislation in their jurisdiction. India is no exception.

transaction of such information. US impose State responsibility to where State collects information and private entities responsibility to their actions with individual information. EU differs from the US to a great extent to that it makes State primarily responsible for protection of data irrespective of the party in the gaining end, be the State or any other entity.

China has adopted a consent-based framework for the general and citizen-oriented purposes. However, it has strict regime from the view point of national security and cross border sharing of information. Data sovereignty is a stressed factor[24]. It focuses on collective good over individual good and ascribes most of data protection duty to cyber security laws.

Right to privacy in India has not been granted expressly in Constitution. Judicial pronouncements including the famous Puttaswamy case[25] brought privacy as a constitutional right under the ambit of Art.21 of Constitution. The right to privacy that was guaranteed to the citizens brought the debate of privacy- of person, as a subject and his information, as an object. In the twenty first century, most of functions of the Government and private institutions require information of the individual to serve the needs of the subject effectively. The information received is processed, stored, retrieved and transferred using computer as a medium. The growth of information and technology that has intensified the need for an effective legal framework.

In India, processing of electronic data has been covered in the Information Technology Act, 2000. The Act under Sec.43A[26] brought a new set of rules called the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI) to primarily govern personal data transfer that is made by body corporate. However, the rules had wide range of shortcomings with rapid technological expansion

[24] Major reason for success of data sovereignty in China is its closed economy.
[25] Right to Privacy Puttaswamy case name and citation.
[26] Body Corporate to be liable for breach of data in case of harm caused

including lack of coverage of new players involved in information transaction[27], the nature of information that gets protection and the narrow imposition on body corporate that excludes State in its ambit.

Therefore, it became a prerequisite to bring about a legal framework that provides liberty in processing information when required, mandates consent to use such liberty and a strict regime where harm is rendered to individual through computerization of information. Hence, Indian requires a framework that should in essence adopt a path which has the combination of ingredients. Legislation should quintessentially consider individual interest as a focal point of protection but necessitate compromise to maximize common good.

3.3 Chapter 2- Jurisdiction and Applicability

The chapter has its coverage to identifying the scope and application of Indian Data Protection Law by cross references to other nations. It specifically focuses on transfer of data in a seamless manner while abiding to its international obligations and also tries to fix liability on the entities and individuals accountable for their actions.

One of the initial attempts to fix issue of jurisdiction has been taken by Organisation for Economic Cooperation and Development (**OECD**) in 1980 where it released an international instrument 'Guidelines Governing the Protection of Privacy and Trans-border Data Flows of Personal Data'. Privacy protection principles propounded by the guidelines primarily endeavoured to consider cross-border data movement and applicable laws to sought issues of jurisdiction.[28] At the core it contains informational self-determination. The same was adduced by the Puttaswamy case and formed the core in Indian privacy and data protection context.

OECD guidelines define personal data as one that contains information that could directly be attached to an individual and further focuses on the movement of such personal data across

[27] Data Subject, Data Fiduciaries, Data Controller are not covered expressly or by implication
[28] http://www.oecd.org/sti/ieconomy/49710223.pdf

national borders.[29] Intangibility is the core of data and the prime reason why the same cannot be traced to a physical location. With technological advancement data could be stored in servers, cloud and their accessibility are not limited by the territorial borders. The accessibility has become directly proportional to the more abstract but deeply connected interconnecting world factor called the internet.[30] No two countries in the global shrunken village possess a similar data protection regime and have decided to rule the flow of data within borders according to their domestic legislations with due respect provided to international law.

The existing laws regulating data flows to a minimal extent has vague applicability and coverage. The vagueness leads to numerous problems considering the possibility of multiple jurisdiction presence for a data at any given point of time. The proposed framework and the Report propose to cover data processed by *Indian entities having presence in India* and with all *entities dealing with personal data of Indians*. Therefore, the framework proposes to extend its arm to outside territories when their entities are engaged with data of Indians.

Jurisdiction and extra-territoriality are pertinent issues due to the fact that data of an individual could be processed anywhere in the world and have no physical presence within a given territory.[31] Arguments favouring extra-territoriality considered the substantial interest of the State to cover companies not based in India but obtain information and data of citizens of India. Arguments against extra-territoriality are that the extent of protection could be in conflict with competing obligations and interests. These obligations would transgress into other jurisdictions which require a co-regulation model to govern the location-less data.

[29] OECD Annex Part 1- Defintion (1) (b), (e)
[30] https://www.aaup.org/sites/default/files/files/IntangibleAssets.pdf
[31] Cambrige Analytica and issues surrounding the same

Stress have been laid to protect personal data of those in India and to provide for a fair compliance mechanism for the fiduciaries operating in multiple jurisdictions. Understanding the prerequisite powers is essential to lay down jurisdiction. The requisite powers are three-fold: Prescriptive, Adjudication and Enforcement requirements.[32] To ensure privacy of information and to protect data of those in India, it is important to table the rules, regulations or law to that extent. The law that is tabled should be capable of being settled in the Court or should possess a possibility of Out-of-Court settlement. Prescription and adjudication should be supported with proper enforcement without which there is no guarantee of justice being rendered to the required information or data that was sought to be protected. The principles are interdependent in nature and are qualified by one another.[33]

Of several principles of prescription, two principles were utilized to ensure protection of data in India. First, the territoriality principle attached with the nationality principle. Data though is indivisible and intangible, could be reduced to a physical entity. Such attachment of data to an entity is typically happens through tracing the location of the server that receives the information.[34] In case of entity being incorporated in India or the individual is an Indian, using subjective territoriality, jurisdiction could be attributed.

On the other hand, data protection regime falling under the private law regime, party autonomy could be guaranteed to decide the dispute using forum selection clauses in the agreement/contract.[35] Situations where conflict of jurisdiction arises due to non-selection of forum or issues in forum selection clause, rescue could be obtained from conflict of laws, transnational treatment and comity of international principles. Instances of such nature call for a test of substantial connection, minimum contacts and the effects that are felt in that

[32] Karnika Seth
[33] Three principles are interdependent
[34] Territorial principle
[35] Party autonomy

particular jurisdiction.[36] It is a plausible effort to address concerns invoking international laws and conflict of law provisions. However, due care has to be taken to ensure laws of other jurisdictions are not encroached upon since resolving conflict of laws may not necessarily apply to laws of all jurisdictions involved in the given matter. Further, implementation of decisions against foreign entities that do not have physical presence in India requires an enforcement arrangement or bilateral negotiation. Adequate representation to the enforcement outside the territory has not been made apart from the general references to soft rules, comity and international norms.

Vast jurisdictional powers vested with the Indian Courts could be identified through the extra-territoriality that is attached by the report. It extends to processing of data of those present in India by Indian companies irrespective of where they are processed. The term 'processing' in turn includes range of data apart from the so-called sensitive personal data. Hence, the scope of the report is largely widened to incorporate actions against processing of non-sensitive personal data or information.

Extra-territoriality marred with such wide configuration to non-sensitive data would lead to issues in sovereignty claims since information actually be processed by the said company as it is possible that only the country of incorporation is India, but the subsequent processes belong to another jurisdiction. Further, the report recognizes *standard of fairness* as an adequate standard to resolve jurisdictional conflicts. Varied facts, circumstances have proved that the fairness doctrine is a subjective one and provides for wide discretion in the hands of judiciary and the executive. Hence, there is a need to deliberate and delineate clear criteria to use fairness as a parameter to address jurisdictional issues.

[36] LICRA v. Yahoo! France Case (Indian Case)

The committee also recommends that personal data of *persons present in India* would be protected. Those present in India is a phrase of wide conjecture to anyone present in India, at an individual level, it be an Indian citizen or resident or not. It also encompasses in its scope, any data fiduciary it be incorporated in India or abroad. It also covers such entities and location where the ancillary and further processing takes place. Such wide encompass might attract multiple laws of different jurisdiction to be applicable which in-turn would result in a situation of conflict with laws of other jurisdictions.

Interestingly, the phrase is followed with an exemption to not extend its arms to protect data of foreign nationals and data that was processed within the India or by an entity that is incorporated in India. It primarily attracts the business processing outsourcing industry present in India that processes data of foreign nationals, on the condition that no personal data of Indians are collected or further processed here. The exemption follows a presumption that the data of the foreign national would be protected in their territory under their respective data protection laws. However, an area of concern is when there exists no data protection law in that other contracting state. Such instance would substantially affect cross-border flow of information and data.

The report though focuses on economic presence, significant commercial stand in processing the data, has also addressed concerns of profiling. It considers profiling to be processing of data irrespective of lack of economic angle to it. Meanwhile, it has brought exemption to information that was collected from untargeted audience or which is purely incidental or accidental. The exemption sought to encourage foreign websites to not to abide by the strict provisions of Indian data protection regime. Such exemption is applicable only when there is no substantial effect or harm in the data collection or processing of data. This is in tune with online economy a free environment without burdening with compliance issues.

Not targeting irregular collection of data is a welcome step in the Indian data protection regulatory regime. However, caution has to be taken to ensure that the small-scale data collection overtime does not result in sizeable amount of data in the hands of the other party. Given the scenario where the Indian data protection laws would have only prospective application, the law might not be able to bring such irregular or ad-hoc collection of data at the later point of time. Yet, it would pose a problem when such small-scale data collection overtime lead to sizeable amount of information and then retrospective effect of the law may not be possible if the data is no longer available with the fiduciary. While protection need not extend to data no longer in existence, it still poses a problem for the time period that it was in existence and yet the law was incapable of protecting it. Another issue in this regard is also the exact definition of small-scale information is not given, and the kind of insignificance attached to the same is not clarified. This can lead to further confusion and it is also unclear as to with whom the discretion for this lies.

3.4 Chapter 3 – Processing

The chapter provides for processing of personal data and individual autonomy over such processing. It considers consent as an end rather than the means to achieve data protection. Careful consideration for the definition of personal data as well as sensitive personal data and the heightened protection that must be afforded to the same forms the crux of the chapter. Another main aspect that was looked into was that of consent. It requires that consent should be – freely given, informed and specific to the processing of personal data.[37] Notice was also considered to be an important part, therefore for bettering the system there were suggestions of better notice design and use of consent management architecture.

As regards processing of data of children being a vulnerable group, some suggested that there needs to be a separate law for the same, despite the provisions entailing parental consent.

[37] Sec.12 of the Bill

This can also be problematic as mere parental consent may not always prove to be the right choice, and therefore a law must be made so that other options besides parental consent are also explored.

The committee recognized that data is no longer in binary states of identifiability and non-identifiability. The degrees of the same may vary. Also, from a set of anonymised data, it is possible to identify the individual. However, the committee also recognized the issues in demarcating which data to protect and which not to, there is a broad import of the definition of personal data. When there is direct identification, protection must be granted. In case of indirect identification, if there is a possibility of being identified, then in that case, protection must be granted as well. However, since no particularly worded definition is being laid down, it can be raised as an issue, especially until precedents are created in order to be followed.

The committee does confer a responsibility on the DPA that they must regularly provide guidance and improve upon the standards and definition of what may be covered under this definition. It has also been given the function of determining standards for anonymisation and data sets that need to be compliant with the law. It is felt that by following a general standard, the DPA would be sufficiently guided. However, it is also pertinent to note that the DPA is an authority to whom such a function is delegated, which forms the basis of this law in the first place. Therefore, it is also prone to further issues, if left unregulated.

As regards sensitive personal data, the above challenge of excessive delegation to the DPA does not take form as the committee itself has delineated certain grounds as necessarily sensitive, therefore the DPA may take guidance from the same. Further, the committee observes the issue of consent, as to how it has become merely boilerplate in the internet world today and therefore, opposed to the very principles of consent. Therefore, it was

suggested that practical difficulties occurring in the same may be removed and it may be made more efficient.

There is a suggestion of treating online consumer contracts as a product in themselves, as they offer no bargaining power to the customer as in a general contract. By invoking product liability, there is a high chance of disincentivizing as the e-commerce companies acting as data fiduciaries may not be ready to bear the burden of product liability when consent is what was sought to be obtained from the said contract. However, it also serves to be an efficient mode as there is a linkage between defects between traditional products and an e-contract which might cause harm to the data principal due to data fiduciary's non-adherence to terms of the notice. Another important positive aspect to the suggestions given is providing requisite granularity thereby allowing data principals to access services without necessarily consenting to all or nothing.

There may be standard model forms laid down by the DPA or compliance with prescribed standards, data trust score for fiduciaries and dynamic consent renewal are a few of the suggestions put forth by the committee to enforce the revised framework. Consent should consist of five qualities – *free, informed, specific, clear, and capable of being withdrawn*.[38] However, this is not a blanket rule as sensitive personal data may require a higher standard of consent. A heightened standard for the characteristics of *informed, specific and clear* must be laid down wherein explicit consent for processing of sensitive personal data is obtained. Consent fatigue is when excessive consent requirements desensitize individuals towards consent itself. To avoid this, a consent dashboard is suggested to keep track of the consents given.

[38] Sec.12 of the Bill

With regard to processing of data relating to a contractual obligation, it is prone to misuse because the data fiduciary might insert additional clauses of unnecessary processing in order to fulfil the contractual obligation. The committee does try to mitigate these risks by opting to treat consent as a ground for processing even though such data is required for fulfilling the contract. However, the issue again here is that if consent is refused, the legal liability in withdrawing from the contract needs to be borne, which does not entirely solve this issue. This merely makes consent forcibly made to be given in a way, for refusal of the same amounts to another liability.

Under determination of how old an individual must be to covered as a 'child', the committee has gone with 18 years as is the age to contract under the Indian Contract Act, 1872. This is opposed to the US approach of treating those below 13 as children, while EU GDPR mandates 16 years, allowing states to reduce the age to 13. Many individuals above a certain age and below 18 years may not even indulge in those online contracts which require extra protection such as YouTube for kids, or other children-centric applications. This would mean that consent for data sharing will be taken over by other individuals merely because the consent given by an individual under 18 years of age would not be taken.

Age verification mechanisms coupled with parental consent for protecting children from harmful effects of data processing such as targeted advertising, tracking, etc have not been substantially laid down, as this suggestion itself may fall prey to its inherent weakness in enforcement. Where guardian data fiduciaries have certain obligations that data fiduciaries need not necessarily follow, there could be an inconsistency in efficiently protecting the rights of children.[39] Furthermore, there is a lack of clarity in the report as to how processing needs to be done in the best interests of the child, and left to the courts of law to deliberate upon.

[39] Sec.23 of the Bill

In the context of community data, the committee urged the Government to create a separate legislation to protect Big Data through class action for certain kinds of data breaches. It also recommended that there be a specific protection for future corporate data in the near future. However, this means that this is a deviation from the proposed data protection law being sector-agnostic and it is unclear as to how these proposed laws are to be formulated.

It was also observed that while the State must be brought within the remit of the data protection regime, there are exceptions to it in terms of national security, investigating crime, protecting revenue, etc. This is dealt with in detail in a subsequent chapter. However, keeping in mind this exclusion and the recent MHA notification allowing ten government agencies to have access to data for the purposes of national security may even go against the approach to a robust data protection regime.[40]

3.5 Chapter 4 – Obligations of Data Fiduciaries

The fourth chapter of the Committee provides for obligations that the data fiduciaries are to discharge while protecting personal data.[41] The Bill suggests that basic obligations of fiduciaries are be laid down to prevent abuse of power and to ensure fair and reasonable processing.[42] Fairness and reasonableness form core of the obligations. However, what is fair and reasonable to the fiduciary may not be fair and reasonable to the principals. It has empowered the DPA and the courts of law in the future to determine what exactly may be considered fair and reasonable processing between a fiduciary and a data processor unconnected to the individual directly, but is performing a function mandated by the data fiduciary in order to fulfil the latter's obligations.[43] This misfit leads to an unequal relationship between the principal and the fiduciary while processing individual personal

[40] https://saveourprivacy.in/blog/explainer-how-the-mha-notification-is-another-step-in-making-india-into-a-survelliance-state-saveourprivacy
[41] Chapter II of the Bill
[42] Sec.4 of the Bill
[43] Committee Report, Chapter IV (B) (I)

data. The report to the extent it warrants duty of care on the fiduciary is weak and without any proper guidelines to decide fair and reasonableness.

Test of fairness and reasonableness is to be fulfilled by the data fiduciary while the entity is performing general processing of personal data. The report provides for certain specific obligations to maintain informational privacy whenever necessary. The foremost of them is to provide notice to the data principal to process the data.[44] It also is a testament that the consent taken for creating a legal relationship may not be sufficient to disclaim liability. The Committee proposes principle of purpose specification which mandates that the fiduciary should specify the purpose for which personal data is collected.[45] It also provides use limitation which proposes that the data should be processed by the fiduciary only for purpose for which it is collected or for reasonably expected connected purposes that could be expounded.[46] Too often the notices relating to obtaining consent or purpose specification or use limitation are either too vague and fail to be specific or be too long winded to be read by the consumer. Such notices fail to fulfil the purpose of specificity as suggested by the Committee Report. The committee and the Bill fail to provide a solution for unclear, long and vague notices. Due note has not been provided for the principle of data minimization which requires that the data collection should be kept as minimal as possible for purposes of processing.

Data maximization is frequent in the processing of Big Data, wherein large amounts of data, not necessarily personal, are collected in order to give a predictive behaviour or targeted advertising, and related purposes. It has been noted that since Big Data is probabilistic in nature, incorrect targeting may lead to inaccuracy of personal data ensuring denial of service and discrimination. The Committee suggests to resolve such issues through anonymization so

[44] Sec.8 of the Bill
[45] Sec.5 of the Bill
[46] Sec.6 of the Bill

that re-identification is not possible and by employing reasonable standards of fairness in using the data for connected purposes and narrow tailoring of use of personal data.[47] The Committee holds the belief that if personal data is being used for targeted advertising, then consent for the same must be taken from them. However, it again confers the decision to the DPA in order to implement this.[48]

Regarding the transparency objective, the committee suggests that a notice should be given by the fiduciary to the principal detailing information about the data that is to be processed and how. However, the committee excludes the same procedure from being followed where processing takes place for emergency situations requiring prompt action, without neither providing an alternative nor defining what would constitute as an emergency situation.

The principle of organizational obligations on data fiduciaries has also been detailed as critical components. All data fiduciaries must be imposed with baseline minimum obligations at least, including implementation of appropriate security mechanisms for individuals to access their personal data. It also provides for access control obligation, through which it is ensured that all data accesses are legitimate and do not violate any substantive provision. This means that all data processing and access requirements are to be scrutinized *a priori* and *ex post* through audits.

Furthermore, the time period till which the data is stored requires re-examination. Once the purpose is completed, the fiduciary must either erase or anonymize the data of the principal[49]. Firstly, data erasure must be through means deemed effective as any resurgence of the same should also be brought within the ambit of data protection. Therefore, the experts must also determine whether anonymisation is the more effective choice of the two and must be

[47] Sec.3 (3) of the Bill
[48] Sec. 61 (6) (m) of the Bill
[49] Sec.10 of the Bill

followed. Secondly, the periodical audit of the data no longer required must be done by the fiduciary, which needs to be held accountable for the same. Otherwise, compliance with this principle may not occur. Thirdly, this may disincentivize fiduciaries as it may incur additional costs, therefore, that issue must be countered in order to protect the interest of developing a free and fair economy. Fourthly, where the overriding effect is given for certain legal or sectoral purposes, such purposes must also come with a time period after which the obligation to retain information must expire. Fifthly, as it is possible that fiduciaries may retain data in order to provide connected services, a uniform expiry date must also exist for allied services to erase/anonymise the data.

The principle of data quality has also been stated here ensuring that the data provided is accurate, complete and kept up-to-date.[50] Notification of data breach is to be made to the principal ideally to shield them from the ensuing harm. However, the committee notes that informing about such breach to the individuals directly might lead to adverse publicity and avoidance of liability on part of the fiduciaries.[51] Therefore, the committee envisages that the DPA must be informed in such cases of breach, before the individual is informed. *Firstly*, this may be flawed as the fiduciary may not, in common-sensical probability, inform the DPA about its own failure just as much as it would not be willing to inform the data principals about the same. *Secondly*, this creates a delay in the principals acquiring the knowledge of the breach and may contribute to their inability to protect themselves from the same.

The definition of personal data breach is envisaged to be structured in such a manner that it focuses on three aspects, or any combination of the same– confidentiality, integrity and availability.[52] Since the committee also notes that not every security incident may qualify to

[50] Sec. 9 of the Bill
[51] Sec. 11 of the Bill
[52] Sec.32 of the Bill

be a breach, there is a requirement for a rather inclusive definition to broaden the scope of this definition, in accordance with established standards.

The committee is also not able to clearly provide the distinction between what may constitute a harmful breach affecting rights of data principals and thereby warranting a notification to the DPA and what may not be of such gravity. Therefore, it puts the burden on the DPA to offer suitable guidance on what action is to be taken in this regard. The committee also does not recommend that benign breaches be notified, which can also be problematic as the self determination of the gravity of the issue is flawed.

The notification from the DPA to the affected individuals during a breach will be decided by the DPA itself, depending on the severity and how the same may be communicated to the individuals. Since in some instances of the breach, the individuals also need to take action to protect themselves from harm, the process adopted by the DPA may not necessarily be efficient, considering the efficacy of the institution.[53] Therefore, the procedure required to be followed may not yield to the fulfilment of the objective of this law. Finally, the security measures are laid down in order to protect data, including through physical measures, organizational measures, and informational measures.

3.6 Chapter 5 – Data Principal Rights

The right to confirmation to the principal has been laid down in order to ensure the data principal is aware of what personal data is with the fiduciary so that their rights can be enforced. However, this may be an expensive process, for which the data principal may be charged reasonably by the fiduciary. This has an exception, wherein all personal data relating to the data principal that has been collected by the data fiduciary must be revealed free of cost, while other factors such as purposes, entities to whom it is further disclosed, etc may be revealed after payment of a prescribed free. This can also be problematic, as the imposition of

[53] Sec. 32 (2) of the Bill

a fee may discourage the data principal from exercising their right or they may also be unable to pay the same. Therefore, flexibility may be adopted in this regard. Time period to the fiduciaries may also be prescribed through delegated legislation to comply with the access requests. Furthermore, in order to comply with the requests, proper care must be taken in assessing the identity of the individual requesting for such information, or protection of identity of such individuals who may seek such information. This has not been addressed in the report.

Right to correction of information if deemed incorrect by the principal must be given to the principal free of cost in order to have up-to-date and accurate information in the possession of the fiduciary.[54] When output personal data (such as a profile) has been created by the fiduciary on the basis of the input personal data given to it by the principal, the same must be notified to the principal to verify with them about the correctness of such conclusions– a point which has not been addressed in the report.

It is further given that the right to object to lawful processing on unenumerated grounds can be vague and thus cannot be provided. The committee has also concluded that with respect to objection to direct marketing, data fiduciaries may only engage in direct marketing on the basis of consent of the data principal. It was also felt that the right to restrict processing need not be given as it is for gaining interim remedies against issues such as inaccuracy of data.

Another set of rights to object relate to objections towards automated decision making and to access the logic behind the same. This right seeks to interject the automated process with a human review so as to prevent from inaccurate output data being presented. However, this is also not immune to prejudices. Therefore, the committee suggests that there be an

[54] Sec. 25 of the Bill

accountability mechanism to weed out such discrimination. However, this does not find an explicit mention in the Draft Bill of 2018.

In the third set of rights, there is the right to data portability. This right allows data principals to obtain and transfer their personal data stored with a data fiduciary for the data principal's own uses, in a structured, commonly used and machine-readable format.[55] Thereby, it empowers data principals by giving them greater control over their personal data. However, data fiduciaries would not be obligated to provide data portability if they are able to prove that technical capabilities as currently existing would make the required access or transfer unfeasible. This code may be set through the DPA so that unnecessary denial of data portability does not happen.

The right to be forgotten has also been introduced in this report.[56] This is to be balanced against the right to know for others, on the basis of certain parameters as mentioned in the report itself. Furthermore, it was also noted that such a test must be assigned to an appropriate entity. Intermediaries are also supposed to take down content once they're informed of the same through a law or an order from the court. Also, the breadth of replication of information must also be considered before granting the right to be forgotten, as the content may have already been replicated further. The report directs the fiduciary to inform other fiduciaries of the principal for data deletion.

3.7 Chapter 6 – Transfer of Personal Data Outside India

This chapter mainly advocates the principle of data localization, i.e storage and processing of personal data within the territory of a state to ensure effective enforcement and to secure critical interests of the nation state.[57] Two approaches are compared – of the US and the EU. The US, owing to its exercise of personal jurisdiction over many tech companies and

[55] Sec.26 of the Bill
[56] Sec. 27 of the Bill
[57] Sec.40 of the Bill

therefore storage of data in its country is able to have a free cross border transfer of information. The same cannot be said for the EU which imposes restrictions to a limited set of circumstances. The committee notes that as for India, its interests must be kept in mind, but an assessment must be made as to what types of personal data may be brought under the law, while other types of data may be barred for cross-border transfer.[58] The same is to be determined by the Government after proper consultation with Data Protection Authority as it is beyond the remit of the committee.[59]

It is also observed that personal data maintained in India will always have the protection of this law, but adequate protection must also be accorded to personal data transferred abroad in national interest. There needs to be more clarity given on the kinds of personal data that may justify such extended protection or who may authorize such justification, but the committee is unable to reflect that in the report.

As regards the enforcement of the same, the report recommends that a model contract for such transfers as formulated by the DPA be followed. However, it also provides for green-lighting of certain countries for free data transfer, through which the committee feels a harmonious balance can be achieved. This can also be flawed if this were to apply as a blanket rule to transfers of all kinds of personal data. Therefore, sector-specific laws or agreements may be entered into.

The committee also recommends that in order to protect the autonomy of the principal, transfers based on consent must be also permitted. By its own admission, the committee realizes that there may be problems in effecting this, but fails to provide a solution. Furthermore, the report analyses the exemptions to free transfer of data outside, where it

[58] Chapter VIII of the Bill
[59] Sec. 40 (1) of the Bill

believes India must adopt a middle path between minimal restriction (followed by the US) and the range of strict laws disallowing the same.

The first benefit referred to is that of enforcement, allowing effective enforcement of local law on locally stored data in a quick and easy way, to effectively secure national security and public safety. Arguments against this were also considered. First, the compliance of outside jurisdictions will be time consuming as they happen through an MLAT request, as per the report. However, one might also consider the possibility of ease of transfer through the technology of cloud sharing. One can also consider bypassing of the MLAT procedure by having effective agreements between countries which often might possess data of Indians. Second, a conclusive cost-benefit analysis must be conducted before the question of costs of imposing data localization is considered by the committee. Third, the committee also notes that "the law will not be enforced" is not a justification as enforceability depends on local enforcement capacity and prioritization.[60]

There could arise a conflict of law situation regarding jurisdiction, which is another issue that needs to be resolved. However, the committee feels that there are more benefits if data is locally stored. This may not stand true for all kinds of personal data, therefore one also needs to look into what types of data may actually be stored locally mandatorily, while what may be allowed cross-border transfer – in order for India to take the middle path.

The second benefit is that of preventing vulnerabilities of breach due to undersea fibre optic cable network. Again, the same argument for blanket applicability to all kinds of data can be invoked here as well. The third benefit is that this contributes to formation of an AI ecosystem by attracting foreign direct investment and the positive impact of server localization. However, this does not mean that data should only be exclusive to India, as one

[60] Chapter VI- B of the Report, at pg.88

copy of personal data may be stored in India while allowing for other copies to be transferred outside of India. An exemption can be with regard to critical data. The fourth benefit is prevention of foreign surveillance with regard to information pertaining to security and other related aspects. While this has the potential to cut off India from rest of the internet world, the committee recommends that only critical personal data should be exclusively processed within India.

The chapter for the purposes of cross border transfer refers to two kinds of data, one being sensitive personal data and other being critical personal data. It is mandated that data fiduciaries are to compulsorily serve a copy of personal data in India in case of cross-border transfer.[61] The process of saving a copy in India is termed as data mirroring. However, data transfer for certain data termed as the critical personal data could not be transferred outside the nation[62] except as may be exempted by the Central Government for purposes of necessity and strategic interests of the state.[63] One of the major issues in drafting the provisions is that it fails to define what constitutes a critical personal data and what situations could be considered as strategic interests.

As regards costs to this, the first one discussed is the economic and market implications. The high cost may be acceptable to large companies, but not to medium or small companies, thereby constructing an entry barrier and further leading to monopolization by the big companies. A middle ground may be achieved in order to facilitate international flow of services and may also pave the way for small Indian data processing companies. The second cost is that of balkanization of internet and domestic surveillance and censorship. This goes against the ideals of free speech and privacy.

[61] Sec. 40 (1) of the Bill
[62] Sec. 40 (2) of the Bill
[63] Sec. 40 (3) of the Bill

3.8 Chapter 7 – Allied Laws

This chapter of the report focuses on the effect that the data protection law in India would have on other laws and the reformation that is therefore required. The new law to be proposed for data protection inevitably has to co-exist and should be able to supplement the already existing laws. In that regard, the committee called for extensive amendments in the Aadhaar Act. The move is appreciated since it runs in line with the Supreme Court verdict on Aadhaar and issues of privacy. The matter has been considered sub-judice by the committee due to the pending proceedings in the court. The report has not adequately looked into Aadhaar Act and privacy violation and has decided to empower the role of UIDAI in a lopsided manner.

With the 2018 Puttaswamy case, the overall constitutional validity of Aadhaar Act was upheld with propositions of changes wherever is necessary. The judges remained unanimous to declare that the Act could process personal data of the individual in light of targeted beneficial services and for the welfare of the community. It ruled out varied circulars, notifications where private entities involved in processing of Aadhaar data from individuals.64 To do so, the Court referred to the proportionality test. The test used four prong criteria of legitimate goal, rational goal, necessity, balancing need to determine the legitimacy of Aadhaar Act.

In light of the same, it is to be highlighted that the requests of authentication of personal data could be performed by the public authority for public functions as approved by the UIDAI. In other cases, such collection and authentications could be possible when the same has been backed by law of the Parliament. The Bill however has not considered offline verification of Aadhaar data with the consent of the holders. Such instances where processing of data has not yet ripe, should be kept out of the loop of the Data Protection Act.

[64] Sec. 57 of the Aadhar Act was read down that allowed processing of data for contractual purposes and to establish identity by individual by private entities, governmental organisation.

The committee has recommended amendments in the Aadhaar Act to enhance the powers of UIDAI to question unauthorized processing of data by companies. Enhancing power primarily ensures protection of the data principals and to bring about enforcement actions against the violative companies. However, a provision that ensures that UIDAI as a data fiduciary is missing in the report. Given the situations under which Aadhaar Act and UIDAI were formulated, it is of utmost importance to bring UIDAI as a data fiduciary or as an entity within Aadhaar ecosystem. To do so, would ensure that the authority is accountable for its acts, for its breach. It would allow the aggrieved to have a prima facie right to proceed against UIDAI before Data Protection Authority for remedies and redressal.

For amendments in the RTI Act, the following were suggested. The Act is to specify the circumstances in which disclosure of personal information would be a proportionate restriction on privacy, having regard to the object of the RTI Act in promoting transparency and accountability. The circumstances under which such personal information may be denied to a citizen can be if there is any likely harm caused to the data principal due to such disclosure.

3.9 Chapter 8 – Non-Consensual Processing

The chapter is designed to provide instances where data could be processed without obtaining necessary consent from the data fiduciaries. It carves out exceptions in line with the *Puttaswamy* recognition of legitimate state interests in processing required data. The committee proposes an illustrative set of grounds *inter-alia* functions of the state, compliance with law or order of court/tribunal, prompt action, employment, and reasonable purpose. At the outset, consent is the heart of the data protection framework. Taking the requirement of consent for legitimate state purposes is essential considering the national interests that might be at stake. However, making it an illustrative list has its own set of drawbacks. The grounds

could be expanded by inclusion by Courts of Law at their discretion. Such inclusion quintessentially would not fit within the legislative intent of the committee report.

Of the five grounds, foremost recognition is provided to 'functions of the state'. The committee observed that there should be sound legal basis to invoke the ground of state functions to process data without consent. Classic definition of State is to be borrowed from Article 12 of the Constitution. The ever-changing definition of State and the inclusion of what could be a state for purpose of Article 12 are out of the scope of the present framework. Intrinsically, processing under this ground could be done either for beneficial and welfare purposes or for regulatory purposes that demands state actions. The report cautions collection only for the particular purposes mentioned and nothing outside the scope of the ground. Further, such collection has to be preceded with assessment of extent to which data is required.

The issue in here is the absence of *checks and balances* to address any additional data that would be collected by the State. Most times, unnecessary collection and its effect would be felt not at the time when data is collected but only after dissemination of such data. Hence, there is an inherent need to clarify and lay down explicit standards to collect data, the extent to which such collection could happen, the purposes for collection, the need for collection and the safeguards adopted to protect the collected data. It would also be prudential to ensure that it is under administrative or judicial scrutiny to ensure data collected for state functions is proper. Such government power could also be addressed through increasing transparency with the data fiduciaries, through increasing audit and supervision.

The second ground, for purposes of compliance with law or order of court/tribunal, the word *law* would derive its validation from Article 13 of the Constitution. While considering orders of Indian courts/tribunals, necessarily obligations under contract or foreign law would not be

considered. Even those functions undertaken by private actors acting under the law would not be taken into consideration. Despite, such processing would have to comply with the data protection law nevertheless and would not find an escape from the special laws. Prompt actions in emergency situations form the core of the third instance. Care has been taken to exclude processing of sensitive personal data as the same would not find any relevance to any measures of prompt action.

Beneficial processing of information including employment purposes finds its mention in the forth ground. The committee notes that the relationship between an employer and employee is not one where the attributes of consent (free, informed, etc) might be achieved, due to inherent dependence on the employment. There may also be the requirement to seek consent multiple times which may lead to fatigue. An issue herein is that processing of such data may lead to intended or unintended discrimination since the relationship essentially is that of human beings. Therefore such information may not necessarily be kept out of and free from human prejudice. The clause is also of wider ambit since it does not provide for a specific mention of collection of sensitive or non-sensitive data. Given the wider ambit, if collection of sensitive personal data is included under non-consensual processing it would result in adverse effects.

Apart from the list being illustrative and different grounds being wider in its own designed way, the last ground acts as a residual clause. It covers instances where data fiduciaries might be required to process information for prevention and detection of unlawful activities including fraud, whistleblowing, and network and information security, where it may not be possible to take consent in all situations. Furthermore, processing of information made public by the data principal is also covered under this ground. In the Indian context, efforts have been made to not make it too capacious by providing illustrations of what may be covered

herein. However, this ground has been subjected to substantial debate with the DNA Processing Bill pending to be passed in the Parliament to be passed as law.

Apart from the grounds of non-consensual processing, committee has also provided for exemptions as per law where processing would not require consent. The report provides for exemptions under seven grounds including security of state; prevention, detection, investigation and prosecution of contraventions of law; processing for the purpose of legal proceedings; research activities; personal or domestic purposes; journalistic activities; and manual processing by small entities. The exemptions are not free from their array of issues that requires redressal.

Security of State, a reasonable restriction of guaranteed fundamental rights is positioned under Article 19 (2) of the Constitution. National security, protection of the interests and integrity of the nation is foremost and collection of data for such purposes has been exempted with. What forms security of state and nation's interest was settled by further legislative and judicial interventions. Adapting the same procedure of what primarily becomes the essential state interest in data protection context to be deliberated by Courts would not serve the current purpose. What is necessary and the proportionate of the information that is necessary to safeguard state interest is not delineated in context. Hence, there is a need to clearly define and to prescribe standards what would be covered under the exemption.

Concerns to formulate effective safeguards from abuse of collected data and of the lacunas in the current framework in providing wide ambit for intelligence gathering have been provided for in the report. As of the day, there is not a single general law in the nation that authorizes non-consensual access to personal data or interception of personal communication for the purposes of intelligence gathering or national security. If there are any entities that are

carrying out activities of such a nature without statutory authorization[65], such activities would be illegal as per the *Puttaswamy* judgment as they would not be operating under law. However, recent MHA notification allowing intelligence agencies to have access to information goes against the spirit of the judgment and the report. Though the notification has a statutory backing under the IT Act, there is a need to strike a balance with other civil liberties.

There are varieties of other legislations that either directly or indirectly provides for such access and surveillance measures. The incidental legislations relating to surveillance and intelligence investigation have not been given due care in the report. The Telegraph Act, 1885[66] and the Information Technology Act, 2000[67] contains provisions of mass surveillance which is not adequately addressed by the report. No amendments have been suggested nor does inserting or substituting provisions of Information Technology Act and the Telegraph Act to the extent find mention in the report. The report also fails to take efforts to address issues of surveillance that could possibly be done by non-state actors.

Instances provide that such surveillance have been dealt with low encryption standards, which in essence risks the data collected. The processed information, their safety standards and the agencies collecting information go unaccountable which does not help in reducing the misuse. Judicial intervention by mandating prior approval from the judiciary to process information obtained through non-consensus could reduce the misuse. Though issues of surveillance and investigation have been properly referred to by the committee, there are no effective measures taken to address the concerns. Hence, there is an immediate need to

[65] For instance, solely through executive authorization

[66] Sec. 5(2)- On occurrence of public emergency and for need of public safety and security of nation- interception of messages transmitted is permitted.

[67] Sec. 69- permits interception, decryption, monitoring of information for defence of India, public emergency or public safety.

oversee and review surveillance by all the wings of the state while adhering to the principles laid down in the *Puttaswamy* judgment.

Second exemption is related to one of the primary duties of the state, i.e., to ensure safety, security, law and order for its citizen. The phrase refers to maintaining public order. Public order finds reference in both grounds for non-processing as well as exemption providing chances of abuse in one way or the other. To investigate and to enforce means to collect, process, streamline huge amounts of personal data. Even the procedural laws of criminal investigations, allows collection and processing of personal data along with other special laws and agencies with similar powers. Here, it is crucial to ensure functions of the state are performed without leaving privacy of the individuals at stake. Therefore, issue arises where data collected is being misused in the hands of authorities, if not supervised and checked properly.

The report states that the personal data of those who are not suspects must be processed for legitimate and well-defined purposes for a limited time only. For sensitive personal data, the rigor provided should be more than just regulatory oversight. It requires procedure established by law to be followed before collection. However, there has been no clarity in the mode in which this might be enforced and the report has sufficiently overlooked the same. In situations of investigation and enforcement, basic required formalities of notice and purpose cannot be followed in its true sense. However, it cannot be left to the discretion of the investigative authorities. Laying down clear standards in the general criminal law or specific legislative enactments or as part of data protection law would help in reducing the autonomy and discretion in the hands of the executive and other authorities.

Non-application of data protection law for the purpose of legal proceedings is the scope of third exemption. The spirit of legal proceedings has been upheld by letting the general right

precede over the special right to be protected under data protection. Research purposes though is an exemption, however is not a blanket exemption. Issues crop in when such research purposes are done for investigation or as a measure of surveillance. The report failed to clearly delineate what may be covered under the said ground to warrant non-application of the data protection law itself. Again this calls for standards that the data protection authority would be able to follow.

Fiduciary relationships, personal and social relationships have been protected with sanctum in the nation. In those lines, information or data that was collected or processed by an individual to cultivate personal or social relationships have been exempted. It is suggested that the exemption is interpreted in its narrower sense as processing of both personal and sensitive personal data carried out for a personal or domestic purpose already enjoy a blanket exemption from the application of the data protection law.

Freedom of speech and expression to media has been a statutory right and the exemption of journalistic activities adheres to the same. It is to apply to the processing of both personal and sensitive personal data. However, conflict could arise in case of two rights, one being right to free flow of information and the right to restrict it for privacy. Hence, the rights are required to be construed harmoniously. Hence, exemption is given to journalistic activities where public interest is overriding. It is also suggested that the media houses adhere to published privacy standards that are considered adequate. Lastly, exemption is provided to information processed manually by small entities which no intention of documenting for large scale commercialization. Such manual processing at any stretch of imagination could not be equated to automated collection of data and hence the exemption is justified.

The cumulative effect of non-consensual processing and exemptions has resulted in a shift in the balance of data power in the hands of the state. Further, the sum total is that there is

increased surveillance that would target innocent data fiduciaries without a probable cause. The vast powers are vested with the government call for more transparency, enhanced supervision and audit that has been overlooked by the committee. While ensuring that national interests are kept at par, ensuring development of citizens without an inhibition is an inherent duty of the State itself. Increased non-consensual processing should be done with proper study of effects, evaluation and a recommendatory sunset clause. What is to be stressed is not non collection of data but usage of data that has been collected through the non-consensual process. It has to be done within the Constitutional and data protection framework safeguarding the value, autonomy and liberty of data fiduciaries.

3.10 Chapter 9 – Enforcement

The chapter focuses on establishment of an authority called the Data Protection Authority who would primarily be responsible to ensure enforcement of data protection regime in India. DPA as an authority is to be established through a separate notification. It like varied other authorities and tribunals have all the powers as that of a civil court including issuing directions, conducting inquires, calling for information etc. It possesses additional powers to bridge the gap between the law and actual practice. There are certain suggestions in the report, such as maintenance of a data trust score, data protection impact assessment and data audits. Offences, penalties and compensation have also been laid down in this.

DPA has a single authority has been provided with four major departments such as monitoring and enforcement; legal affairs, policy and standard setting; research and awareness; and inquiries, grievance handling and adjudication. It is important to take note that each of the four functions is important and its efficiency is important to have a successful data protection regime. To carry out the four works of the four fundamental pillars, human resource is an essential factor and has been thoroughly overlooked by the Committee. There is heavy burden imposed on one body without giving due consideration to the fact that such

an establishment would for the first time see the light of the day. The authority would have an intake of six whole time member and that does not seem to fit into the effective scheme of functions that the authority was rendered to do. Also, appointment of members possesses major governmental influence which takes away the autonomy of the authority.

The authority would act as an adjudicatory wing to settle issues or conflicts in data protection. The report primarily suggests the hierarchy of settlement of issues of privacy and data protection. Reporting of issues at the first instance would be with the adjudicatory wing of DPA, appeal would be before the appellate tribunal with further appeal to Supreme Court which would act as a court of last instance. Taking away the powers of supervisory jurisdiction of High Courts as provided in case of L. Chandra Kumar v. Union of India[68] is in contravention to the established principle of law. A classification is recommended for significant and other data fiduciaries, wherein the former will have additional importance and they will be tracked separately.

Apart from establishing what amounts to an offence and what would be the penalty imposed, the report fails to provide what are the possible consequences of non-compliance of the regulation. As the title of the report goes, to unlock the free digital economy, it is important at the first instance to not to proceed against claims but to provide adequate warning of the possible infringement and non-compliance. Warning should be issued at the initial stages when not much of the information and data is under threat. Instances of breach of warning should be followed by sufficient notice to proceed against the offender in the courts of law. In case of failure then monetary compensation should be imposed with looking into varied factors as listed by the committee. However, when the harm caused is so grave that it is against the public policy, contrary to the laws of the land, and then there should be a

[68] AIR 1997 SC 1125

temporary or definitive ban on the organization for processing of data in addition to the monetary compensation.

When the individual could be traced to by lifting the veil and is found the sole person responsible for grave offences, it is suggested to proceed with criminal actions against the individual similar to the criminal provisions against directors under companies' law. All the penalties as imposed by the DPA should be in proportionate to the offences committed, be effective and dissuasive. Deterrence theory of punishment could be followed considering the importance of protecting the data of individuals of one jurisdiction in multiple jurisdictions. Action taken must be a corrective tool for the organizations to act in compliance with the data protection laws.

Indian data protection law in addition provides a long arm to proceed with extraterritoriality. International standards with the present day cross-border transactions have increased the reach of domestic authorities to other territories where the offender is located. However, data regulation in India is still at its nascent stage and so does the enforcement process in India. Therefore, it is to be tested how the data protection laws of the nation would regulate and enforce its claims in cross-border cases. The committee report fails to address how the framework would shape in cases of multi-jurisdictional misuse of data. Though the report provides for penalties to be imposed for any offence committed in India or outside India but of those persons located in India, there are no clear set of penalties prescribed. It is suggested that the standards set in capital market regulations in India could be followed. Imposing the highest of the penalties or three times worth the financial gain that the offender would gain through the harm would be effective to ensure adequate data protection of persons in the nation.

Despite challenges, the framework proposed is welcome and it is important for any person to ensure compliance of the same. Organizations located in India or outside but dealing with processing of data outside India have to look into the application of the provisions. It is recommended that organizations are given sufficient time frame to secure the data and to enhance their infrastructure. A period of six months could be afforded considering the sensitivity of both the organization and data involved. It is therefore vital for organizations to take note of appropriate compliance measures as required by the law in India.

The committee has been successful in formulating a legal framework for the most complex and controversial areas, privacy and data protection laws. Enforcement is the real challenge in the report. It imposes a question, whether the nation is sufficiently equipped with the means and measures to enforce the rules and the compliance actions against offenders. The data of the individuals could be processed anywhere in the world irrespective of whether the website has a server located or the organisation has physical presence in India through its permanent establishment, fixed place of business or otherwise. The broader ambit of data processing has rather made the claims and needs of extraterritoriality to be attached to the regulation. It is primarily an attempt to ensure that the data protection laws of the nation are not circumvented for any purpose, whatsoever.

The committee has decided that the new law would have extraterritorial effect. It has adduced to following the effects and target test of jurisdiction to proceed against entities that don't have physical presence within the territory. This change brings about the biggest challenge of how the authorities including DPA would effectively implement the data protection standards. With the exponential growth of the social networking sites, cross border communication sites, cloud, it is more than a reality that most of the data is being processed outside the given territory. To apply such higher standards outside the territory, two specific aspects are to be considered. First, the legality behind the claim outside the territory should

be looked into. Later, it is to ensure that the decree of the Court would be enforcement in the state of incorporation of the website/entity.

The approach of the extraterritorial jurisdiction is justified on the basis that the borderless internet, target, solicitation or advertisement of business would be treated with laws that requires no borders. It primarily follows the protective principle for those who are located within the territories of the nation. However, proper care and caution has to be taken to ensure that the efforts taken do not result in attracting foreign business in the nation. Therefore, proper exceptions, claims and guidelines are to be laid out in order to strengthen foreign investments in the economy.

What is pertinent is to identify the right tools of enforcement to ensure success of regulation. To be beneficial, India must ensure that the data protection representatives are able to obtain international cooperation, friendship, harmony, exchange of information and mutual assistance. These tools with enhanced cooperation would help to enforce decisions in a direct way. Achieving best results through direct measures would be possible with the appointment of representatives who would seek consent and cooperation in cross borders. Alternatively, such assistance could be incorporated in contractual clauses or treaty clauses so to avoid issues in dispute resolution and enforcement at a later phase of execution.

However, in recent times, indirect means also prove effective with concepts of incentives of compliance; risk involved in reputation and adequacy norms in other countries. To achieve higher rates of success with direct and indirect modes of enforcement, it is essential to adhere to the rules as laid down in public international law and to respect comity. Further, mutual obligations of parties to enforce decisions are to be adhered in perspective. The committee provides for data audits, data protection assessment within a nation state, to enforce the decisions within the nation. Using target test, similar audits, and assessments has to be taken

with respect to the operators who are active in India. To achieve the best results of such audits and assessments, what is to be encouraged is the concept of retaining the data within the territory.

4. Contextualizing GDPR in India: Analysis of Privacy Laws in India

The European Union has been successful in handling data revolution and has adopted to the transformation by adopting the famous General Data Protection Regulation (GDPR). Given big data, data analytics and instances of data misuse at a larger scale[69,] GDPR has become an attractive option for other nations to look up-to to bring in a national legislation to protect data of their nationals. The structural framework of the regulation contains 99 Articles divided into 11 chapters. GDPR as a regulation is shifted towards heavy compliance, regulation with higher prescription. The regulation considers data protection to be a fundamental right and considers such protection to form integral part of existence of natural persons.[70] To ensure that the fundamental right is not tampered with, the regulation is aimed to provide higher standards of protection to the data subjects.

GDPR is an ambitious legislation in that it does not limit its reach to the European Union. It would apply to enterprises irrespective of the actual location where data is processed. It provides for extra-territorial reach in three instances (a) where goods and services are offered to the data subjects of the nation (b) when data of the subjects are tracked, monitored with the intention of doing business with EU nationals (c) where processing takes place in context of enhancement of activities of the organisation.[71]

[69] Cambridge Analytica and Facebook Connection
[70] Art. 1 (2) GDPR
[71] Art 3 GDPR

Given the fact that India is in active process of bringing about law relating to data protection, it is indispensable to consider the necessary template of GDPR. The Apex Court while rendering decision in the privacy case discussed different progressive data protection principles of USA and EU data protection regime.[72] Reference was made to the possibility of bringing the Personal Data Protection Bill, 2018 in tune with those principles to bring a comprehensive legislation in the nation. However, it failed to specify the possibility of adoption of any provision in Indian context.

Indian jurisprudence on decision making using data is still at its nascent stage. Repositories of data by corporations and government are yet to be created in India.[73] In the given set of circumstances India cannot afford to adopt such high standards of data protection regulation as that of European Union. However, it is advisable to incorporate those provisions to bring an effective data protection regulation. The reasons for contextualising GDPR in India are multi-fold and inter alia includes the following:

- Thoughtfulness in adoption of GDPR provisions would help in not bringing about new changes in the legislation of data protection.
- It would help Indian industries to enhance the business connection with European States and a sui generis protection to Indian businesses abroad.
- It would help the nation to adapt itself to the faster changes in technology.
- Incorporation of required principles would bring in robust laws and reduce judicial inclination to adopt data protection principles of other jurisdictions in deciding cases relating to data protection.

[72] Privacy and Aadhar case
[73] An exception being the AADHAR Act, 2016

4.1 Right based Model

GDPR is enacted with consent as the means to achieve the end called data protection. It upholds the legality of data processing only when the data subject is informed about the purpose of collection. It is inherent requirement that the data subjects have consented to the required purpose.74 On obtaining consent to process the information, the data controller holds different ways in which the data could be processed. Most of the privacy policies that was updated post GDPR explicitly include that the controllers are free to use, process and share the data with the third parties after obtaining the consent of the user.[75] The consent-based model of data privacy therefore has consequence that is beyond the control of the data subject on providing consent to process.[76]

The Bill of 2018 provides that the data fiduciary may obtain consent to process personal data.[77] As opposed to the consent based which provides wide discretion to the data fiduciary, a right based model considers individual and his right to privacy central. It brings in a regime when the data fiduciary would be held liable in the instances of breach of the right of the data principal. It enhances the responsibility attached to the fiduciary and judges his actions on a case to case basis.[78] Right based model of privacy would provide for much better autonomy as compared to the consent-based model that is primarily followed in larger part of the data economies. In the right based regime, consent becomes one of the criteria of processing information. Other inclusive rights that comes for consideration include identity, privacy, participation, ownership, due process, freedom of speech and expression.[79] At this juncture it is pertinent to note that RBI has already taken effective steps to use right based approach of

---

[74] Art 6 (1) GDPR
[75] Google Privacy Policy See, < https://policies.google.com/privacy?hl=en >
[76] See, <https://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf >
[77] Sec 12(1) Personal Data Protection Bill, 2018
[78] Privacy as Virtue: towards an actor-based approach to privacy regulation, Dr B Van Der Sloot, See, <https://www.ivir.nl/projects/privacy-as-virtue-towards-an-actor-based-approach-to-privacy-regulation/>
[79] See, <http://www.undatarevolution.org/2014/10/14/rights-based-revolution/> UN Data Revolution Group

data protection relating to collection of household financial information.[80] This alternative when considered for purposes of data protection laws in India would address the legitimate concerns of data principals in several aspects.

4.2 Rights of Data Principals

Indian Bill of personal data protection in its Chapter VI provides for data principal's rights. The rights incorporated in the Bill are similar to that of Chapter III of GDPR in certain respect. Both the Bill and GDPR provides for right to access, confirmation[81,] correction[82], data portability[83] and forgotten[84.] The Bill has made it clear that the rights of the data principals are not absolute and could be withdrawn in the interests of the state and for want of necessity for the purpose of data principals or of the state. However, the Bill has certain issues that require redressal. Rights of the data principals could be fulfilled only with proper retention policies that could be used to track the data storage. Prescription of data retention period helps the data principal to be assured that the data would be erased upon specified period.[85] GDPR in its right to access provides for a right for the data principal to let him know of the retention period.[86] A similar straightforward right is evidently missing in express terms of Sec.24 of the Bill. It also fails to provide for a right to objection in case of automated decision making in processing of personal data. However, right relating to objecting automated individual decision making and profiling is found in GDPR.[87]

The Bill has direct provisions relating to right of the data principal to request for a restricted usage of his data. He is also guaranteed with a right to be forgotten in instances of his purpose being served, his consent being withdrawn and when the collection and processing of

[80] RBI report on Household Finance Committee, Appendix F- Right Based Data Protection Framework
[81] Sec.24 of Bill
[82] Sec.25 of Bill
[83] Sec.26 of Bill
[84] Sec.27 of Bill
[85] KPMG International, https://assets.kpmg/content/dam/kpmg/nl/pdf/2018/advisory/data-retention.pdf
[86] Art. 15 (d) of GDPR
[87] Art. 21, 22 of GDPR

the personal data was done contrary to the laws passed in the Parliament or the State Legislature.[88] The right to be forgotten as in the Bill provides that the data would be discontinued from disclosure on the fulfilment of certain conditions. Therefore, the right is more restrictive in nature as compared to the right of erasure that is guaranteed under GDPR.[89] The GDPR rights relating to data principals are wider and more inclusive in nature as compared to Indian Data Protection Bill. Data principals and protection of their rights forms the heart of the Bill. However, narrow prescription of the rights takes away the essence of the legislation, hence calls for a revamp in the same.

4.3 Classifying Data Breach

EU Regulation operates against data breach. It defines personal data breach to be security breach that could either be accidental or intentional.[90] Similar definition that includes unauthorised or accidental disclosure forms part of the Indian Bill.[91] It is therefore evident that actions against data fiduciaries are inevitable irrespective of it being intentional or unintentional on their part. The major reason for such an inclusion could be the impact such incidents cause on the data principals. Intentional data breach is where there is maliciousness and unlawful intrusion in the destruction, alteration or loss of the data. Bad faith forms the core of such data breaches and the regulations imposing such hefty penalties are justifiable.

Instances to that of recent Equifax data breach incident which involved compromise of nearly 146 million primarily due to human error to follow security warnings do not strictly fall under the category of intentional data breach. Given the grave injury to the data principals, the cost that Equifax had to pay for the same was huge.[92] Circumstances which involve breach due to ignorance or technical issue or force majeure where there is no significant harm

[88] Sec. 27 (1) Bill
[89] Art. 15 (e) of GDPR
[90] Art. 4 (12) GDPR
[91] Sec. 3 (30) of the Bill
[92] The Equifax Data Breach, https://www.ftc.gov/equifax-data-breach

or financial loss caused to the principals, it must be classified under technical data breach. In cases of technical breach, it is not likelihood of harm that should be considered rather what is required to be proved by the data principal is that there is an actual damage that has happened in the due course of the breach. This would help ensure that single failures that could be rectified when brought to the notice of the entity is not imposed with huge penalties.[93] Therefore, it is recommended that the Adjudicating Officer under the Bill while considering breach using different factors[94] should also identify whether the breach is intentional or incidental and proceed accordingly.

4.4 Fines and Penalties for Data Breach

Data breach in European Union is viewed seriously and the same is reflected in GDPR. Penalties under the regulation take a stepped approach based on the nature and gravity of the offence. It imposes penalty of up to 4% annual worldwide turnover or EUR20 million, whichever is higher. The penalty extends to non-compliance of basic principles of processing, it be personal data or specified personal data, when data is transferred without due consideration given to adequacy provisions, violating data subject rights and for violating the orders of supervisory authority.[95] It attracts a penalty of 2% of total worldwide turnover or EUR10 million for specified breaches. They include breach of data relating to children, for not maintaining records of data processing activities, holding data without sufficient security measures, for violation of data protection impact assessment, processing of data without proper GDPR certification and not following prescribed code of conduct under the regulation.[96]

[93] Data Breaches – From Accidents to State Sponsored Attacks: Vulnerabilities and Strategic Plans, Paige Backman, https://www.airdberlis.com/docs/default-source/newsletters/privacy-law-bulletin---march-11-2015.pdf?sfvrsn=2
[94] Sec. 74 (4) of the Bill
[95] Art. 83 (5)
[96] Art. 83 (4)

Following the GDPR, Indian Bill on Data Protection also has step-wise penalty depending on the nature of offence. The penalty varies from 2%-4% of annual worldwide turnover of the entities or Rupees 50-150 Crores, whichever is higher.[97] The range and percentage of penalty also differs depending on whether the data fiduciary is significant or not.98 Range of varied offences and penalties start with few thousands of rupees for violation per day. It also held that prescribed criminal offences to be non-bailable along with five years of imprisonment.[99] The penalties imposed in par with GDPR do not provide adequate regards to significant harm caused to the data principals through violations of various provisions of the framework.[100] Here, the distinction between intentional data breach and technical data breach plays a vital role.

It is essential to incorporate harm of the data principals to penalise data fiduciaries in case of technical data breach. This has been advocated in the Bill in sections 90-92. It is therefore inherent to look into wrongful loss or gain to the data principals in case of technical breach which could be rectified and has happened beyond the control of the data fiduciary. The Bill has prescribed penalties for breach done by state actors.[101] However, it fails to provide guidelines to quantify breach done by State and Government. In the instance of government departments contravening the provisions of the Act, computing penalties would be difficult since they do-not fall under the category of having annual worldwide turnover. Therefore, it is important to explicitly provide for penalties computation for breach by government. Since data literacy is major impediment in the nation, it should be ensured that the fines and penalties are utilised to promote awareness and literacy among the general public.

[97] Sec. 69 of Bill
[98] Sec.38
[99] Sec. 93
[100] Sec. 43A of Information Technology Act, 2000 read with SPDI Rules, 2011 provide for consideration to whether the breach caused harm to the data principal or not.
[101] Sec. 96

4.5 Regulatory Body

The Bill of 2018 envisages a separate Data Protection Authority.[102] DPA is the ultimate authority in the legislation to ensure that the data principal interests are protected.[103] For such purposes, they have to entertaining complaints, interrogation, decision making, executing the decision made. They are also provided with a preventive role where they are to ensure that data is not misused and that strict compliance has been properly carried out. To check the same, they are responsible in ensuring that the data fiduciaries are carrying out the data protection obligations, to regulate data breach notifications as required by the law.[104]

In order to best perform data protection propaganda, they are also held responsible to promote awareness to the general public of the importance and need to protect personal data.[105] The functions under the Bill simply overburden the authority without adequate staffing. Further, providing the authority of all respects of compliance from interrogation to decision making to implementation goes against the basic tenants of legal enforcement. In order to reduce the burden of DPA, there is a need to establish a separate Data Protection Board similar to that of the European Data Protection Board prescribed under GDPR.[106]

Data Protection Authority of India not only carries the burden of performing numerous functions. It also lacks independence in the sense that the appointments would be done and regulated by the Central Government.[107] The Bill does not limit the jurisdiction of the Authority and does not provide for a process through which the adjudication wing of the Authority would act to hear and decide cases. Lack of independence would inherently affect cases where the State or the Union is the data fiduciary. Therefore, there is a need to relook into the provisions relating to the appointment of members of the Data Protection Authority.

---

[102] Preamble of the Bill
[103] Sec.60 (1)
[104] Sec. 60 (2) (a)-(l)
[105] Sec. 60 (1) read with 60 (2) (m)
[106] Art. 68 GDPR
[107] Sec. 49 of Bill

4.6 Handling Costs

GDPR promotes transparency in dealing with the data of the data subject.[108] Dealing in here is inclusive of collection, handling, processing and storage. Collection and handling of data has been taken care by companies by drafting appropriate privacy policy in place.[109] Processing and storage of data has been debated due to the cost involved for the same. Reports have estimated that the cost involved in compliance of GDPR in processing and storage would amount to about 7.8 billion dollars for the Global 500 members.[110] It is also estimated that the response costs, i.e., the cost of data breach would amount to 3.86 million dollars.[111] These costs tend to go up with scenarios of minor non-compliance of rules, regulations.[112] Such high costs would eventually lead to business stopping interface with the given territory, in given instance, EU. It would heavily hamper building new business within the geographical limits.

Attracting investments, promoting business, easing regulations has become part of industrial boost in India. Involvement of costs reduces the ease of incorporating business in the nation. It could affect the stake of large business in adopting stringent storage measures. While processing and storage is crucial for an effective data protection regime, Indian perspective towards enterprises and cost reduction in compliance has to be guaranteed. This could be achieved through following means:

- Looking into the purpose for which the data was collected by the enterprise and also identifying the use of the data in entrepreneurship.

[108] Art 12 (1) of GDPR
[109] Websites in India dealing with European Citizens have amended Privacy Policy to the required compliance of GDPR
[110] International Association of Privacy Professionals and EY https://iapp.org/
[111] 2018 Cost of a Data Breach Study by Ponemon https://www.ibm.com/security/data-breach
[112] https://dynamic.globalscape.com/files/Whitepaper-The-True-Cost-of-Compliance-with-Data-Protection-Regulations.pdf

- Considering small enterprises in a different fashion with that of the large enterprise which are primarily into data processing for their benefit. For effective cost reduction, the reserves and logistical capacity of the small enterprise could be taken into account.
- Proper warning, notice and freeze time has to be provided before proceeding with imposing penalties and causing business suffer from non-compliance costs.
- Adequacy Provisions: Transfer of data between borders is a pertinent issue in the borderless internet space. GDPR tackles the issue of cross border transfer of personal data upon satisfaction of two tests: the adequacy test and the comparable level of protection test. Adequacy test helps in identifying whether the third country to which data is proposed to be transferred has adequate laws of protecting the data to be transferred. Decision of adequacy is combined with the proposal of European Commission, opinion of the Data Protection Board, approval of representatives of EU Countries with final adoption by the Commissioners. When the adequacy test is not fulfilled, then comparable level of protection that could be provided by the other nation state. Comparable protection be identified by their willingness to enter into standard data protection clauses of the Commission, with the corporate rules followed, with the approved code of conduct and the certification mechanism.

The Personal Data Protection Bill, 2018 mandates prior approval of Central Government to transfer personal data of data principals to other nations only on fulfilment of adequate level of protection. To understand whether the set of data could be transferred cross border or not, consultation by Central Government could be sought from the Data Protection Authority. The Authority is also imposed with the general functions of monitoring the cross-border data flow. It is also authorised to suspend or discontinue such data flow at a later point in case the other nation does not fulfil the adequacy standards. The Bill though attempted to incorporate the adequacy provision, it has not

prescribed any standard or method through which adequacy level could be determined. There is no proper set of guidance for the data fiduciaries to check adequacy and comparable protection. It burdens the DPA to smoothen the flow of data, to monitor, enforce, take action in case of misuse. Therefore, it is necessary to incorporate certain standards in lines of GDPR to have adequacy provisions of the Bill more effective.

4.7 International Convention

Different nations are actively involved in bringing about legislative framework to protect privacy of individuals and their data. Each nation is focussed in developing a normative regime considering the unique features their geographical, socio-economic situation. Chances of uniformity and stability in the provisions of different national legislations is considerably low. The national laws relating to data protection are posed with major gaps and there are numerous changes that are required in the same.[113] In order to bring in provisions to match with modernisation process, the need of the hour is to frame a multinational agreement/framework.

One of the stand-alone international treaty dealing with protection of personal data is Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981.[114] The Convention is one of the first to outlaw the processing of sensitive personal data. The new treaty to be proposed could follow the lines of 1981 Convention with changes incorporated to include technological changes and that which proposes a universal standard. The OECD Guidelines on the Protection of Privacy, 1980 that was further revised in 2013[115] to accommodate data protection principles for changing times can also providing a guiding light for the new framework. The new framework to be agreed upon by the nation states should be flexible, transparent and robust. While accountability is ensured, the

[113] Privacy International, Data Protection, https://privacyinternational.org/explainer/41/101-data-protection
[114] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108
[115] See,<http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm >

framework should also increase the international compatibility.[116] It should permit opening up of digital economy, allow smooth flow of data, harmonise issues among nations and should contain effective safeguarding measures to tackle instances of abuse of data belonging to other nationals.

4.8 Promoting Data Literacy

Growth of internet and e-commerce has inherently resulted in abuse of privacy and misuse of personal data. The concern of personal data protection was highlighted in a recent collaborative survey of Centre for International Governance Innovation, and UNCTAD.[117] Major reasons for such misuse are the challenge in literacy that takes away the data principals right to request the data fiduciaries accountable to their actions[118]. Data literacy is required to be promoted. Indian Bill though contains provisions to enhance awareness on data protection and data literacy, the method of implementation of such mass awareness is ambiguous and vague. One of the possibilities of ensuring that proper awareness is provided is to ensure that the terms and conditions in the usage of personal data is simpler. Accommodating opt-out clauses in built in the standard form contracts can ensure that data principals are provided with sufficient opportunity in using their right while agreeing to process the data for undertaking the benefits as provided by the fiduciaries.

[116] Morgan Corley, The Need for an International Convention on Data Privacy: Taking a Cue from the CISG, 41 Brook. J. Int'l L. (2016).See, < http://brooklynworks.brooklaw.edu/bjil/vol41/iss2/5>
[117] See, < https://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=1465 >
[118] See, < https://undataforum.org/WorldDataForum/should-data-literacy-be-promoted/ >

5. Approach and Analysis of Privacy Laws in India

Any policy formulated for purposes of privacy and data, should focus on protection of people rather than on empowerment of people through the data economy. It is essential to address the existing challenges towards privacy and data protection to set forth effective regulatory framework that would help organisations and regulators to set a harmony in compliance and enforcement. With privacy being recognised as fundamental right, there is an inherent need to relook into the principles articulated by policy-makers to protect privacy. Till date, there are no effective legislation or privacy principles that provide clarity in the way the data and privacy of the individual is to be protected. Times where economy is digital centric and privacy and data of the individuals are transacted more often for the financial benefits, it is essential to bring in new clarity and a new approach that governs privacy and data.

5.1 Consent Based Approach of Privacy

The privacy and data protection laws around the world has consent at the core of protection of data. The notion finds reflection in the Puttaswamy case, Justice Kaul[119] in concurrence with Justice Chadrachud[120] in their respective pronouncements held that the State should be responsible to ensure that the information obtained from the users should be based on their consent. The information thus obtained should primarily be used for the purpose (purpose limitation) and to the extent of which it is disclosed (use limitation). Consent based privacy model along with the principles of purpose and use limitation found its first discussion in the AP Shah Committee Report.[121] After the judgment, the same finds position in the Protection of Personal Data Protection Bill, 2018.[122] The new law proposed therefore has expanded the

[119] Para 70 Puttaswamy
[120] Para 177 Puttaswamy
[121] The actual report and para numbers
[122] Section numbers

scope of consent requirements to process the sharing of data. With the widened gamut, it also ensures that there is technologically neutrality in the consent-based approach of privacy.

One of the major criticisms of the consent framework has been that it is not easily amenable to change and most of the terms are pre-determined as a boilerplate. Such standard forms do not allow the users to negotiate the complex terms. The user is also left with almost no alternative option to avoid consent. Most of the data fiduciaries require the data principals mandate consent to access their services, which results in the primary purpose of choice redundant.[123]

In the given model, the notice and choice of the data principal is obtained once in the beginning of the entire process of collection, processing and storage of the data. However, with increased access to technological devices, data feeding of the data belonging to the data principals have become a continuous process for which no specific, informed and clear consent is obtained for. This continuous feeding culminates into a data footprint that leaves credibility and efficiency of the consent-based framework with unanswered questions. Though consent allows free flow of data, it also leads to the threat of individual control over data prints in a long run. In situations of continuous feed, the data fiduciaries should adhere to the basic conception of privacy as a right apart from the earlier consent that was obtained. Therefore, to avoid cumulative data footprint and to ensure that the data footprints are provided due protection, it is necessary for the policy-makers to ensure that privacy works both with consent and with right.

Most of the consent requirements operate on a take it or leave it mode. In essence, they are clickwrap agreements where the user either accepts to site-specific requirements before logging on. Mere I accept, has become the consent as required by the legislations which

[123] Contract as Thing by Arthur Leff

though is in accordance with the letter of the law, goes against the spirit of the law. Studies provide clarity on the consent regime where they were effective when the data principals were clear about the organisation that dealt with their information and the reason for the collection.[124]

Major disadvantages of consent-based framework are that they come useful and handy only when the data principal is fully aware of the consequences of the consent provided. Others include the complexity, consent fatigue, the fear of missing out in social interactions, growing family companies, their inter-connected databases along with machine learning and intelligence algorithms.[125] In the given context, where there is no actual direct interaction between the data principals and fiduciaries about privacy concerns, it has become difficult and almost impossible to ensure that the individual consent obtained through pop-ups is appropriate. In a country like ours, the user related awareness is neither self-sufficient nor the attempts to ensure spreading awareness have been futile. Therefore, the data principals tend to make misleading decisions that are not necessarily privacy conscious and has any privacy control over their actions. Therefore, the informed, specific consent-based framework fails to withstand itself as a privacy and data assurance framework.

5.2 Right based approach of Privacy

The law makers are currently facing a situation where policy and legal reforms are required in bringing about data protection norms in India. Various steps, measures, discussion have taken place in the recent times to the given context. All the legal steps are aimed at a mechanism called a consent-based framework where privacy of the individuals is obtained and are easily put to test and compromised without major consequences. Under the consent regime, the fiduciaries are not held accountable for numerous acts and onerous data collection

[124]See, <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/#heading-0-0-6-2>

[125]See, <https://www.livemint.com/Politics/Le4uhieRgGa5PgFiKWH5nM/Why-consent-is-important-in-ensuring-privacy-protection.html>

using consent as a means of collection. Further, the interoperability and increasing transfer of data among the group companies has made it difficult to attribute liability to a particular fiduciary. The regime also fails to holistically protect the individual data rights. These lacunas prove consent model increasingly inadequate with consent fatigue being its characteristic feature.

Therefore, it is needed that the law recommends consequences and harm. The concept of harm and consequence would render effective only on bringing about basic data protection rights. Bringing about rights and establishing their scope, would enable enforcement authorities to establish clear cut violation by the data fiduciaries including the significant and guardian data fiduciaries.

GDPR is enacted with consent as the means to achieve the end called data protection. It upholds the legality of data processing only when the data subject is informed about the purpose of collection. It is inherent requirement that the data subjects have consented to the required purpose.[126] On obtaining consent to process the information, the data controller holds different ways in which the data could be processed. Most of the privacy policies that was updated post GDPR explicitly include that the controllers are free to use, process and share the data with the third parties after obtaining the consent of the user.[127] The consent-based model of data privacy therefore has consequence that is beyond the control of the data subject on providing consent to process.[128]

The Bill of 2018 provides that the data fiduciary may obtain consent to process personal data.[129] As opposed to the consent based which provides wide discretion to the data fiduciary, a right based model considers individual and his right to privacy central. It brings in a regime

[126] Art 6 (1) GDPR
[127] Google Privacy Policy https://policies.google.com/privacy?hl=en
[128] See, <https://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf>
[129] Sec 12(1) Personal Data Protection Bill, 2018

when the data fiduciary would be held liable in the instances of breach of the right of the data principal. It enhances the responsibility attached to the fiduciary and judges his actions on a case to case basis.[130] Right based model of privacy would provide for much better autonomy as compared to the consent-based model that is primarily followed in larger part of the data economies. In the right based regime, consent becomes one of the criteria of processing information. Other inclusive rights that comes for consideration include identity, privacy, participation, ownership, due process, freedom of speech and expression.[131] At this juncture it is pertinent to note that RBI has already taken effective steps to use right based approach of data protection relating to collection of household financial information.[132] This alternative when considered for purposes of data protection laws in India would address the legitimate concerns of data principals in several aspects.

In the consent regime, after the initial consent is provided, it becomes the burden of the principal to identify if the data is processed for further purposes. This burden of proof on the individuals lets the principals to escape from liability and further consequences. In the right based regime burden of proof is eventually shifted on the data fiduciary in place of data principal. The shift brings with it on the data fiduciaries a mandatory compliance of data processing standards and prescribed legal norms.

Take it or leave it clauses should not be encouraged even in consent-based model. This being said, the clauses should have the negotiating power with more power being vested with the data principals and not with the fiduciaries. Further, in a consent regime, the individuals are faced with a scenario where the principals denying consent for certain clauses results them in obtaining the services from the data fiduciaries. To the contrary, the right based regime

[130] Privacy as Virtue: towards an actor-based approach to privacy regulation, Dr B Van Der Sloot, https://www.ivir.nl/projects/privacy-as-virtue-towards-an-actor-based-approach-to-privacy-regulation/
[131] http://www.undatarevolution.org/2014/10/14/rights-based-revolution/ UN Data Revolution Group
[132] RBI report on Household Finance Committee, Appendix F- Right Based Data Protection Framework

should provide due care for such instances. These granular aspects could effectively be taken care of in the rights regime, since access and availability of services would be considered as a right of the individual.

The right based regime does not only look into access to services but also at a large-scale providing protection in case of harm being caused to the data principals. It calls for proper due diligence by the data fiduciaries and processors. Where due diligence fails and mishap occurs, the fiduciaries would be liable, resulting in rights providing a better shield compared with the consent. This protection mechanism would also ensure that the rights of the controllers are not placed much above and in a better pedestal than that of the principals. Three core principles that would form an effective regime include the accountability of the data fiduciaries where harm is caused. Second is the autonomy that the individual has to bear and the decision-making power in the hands of the individual rather in the clutches of the controller. Finally, and most important is the safety and security measures that are undertaken by the controller to protect the data that is collected from the principals.[133] In the absence of accountability, autonomy, security, then, the right-based regime would not achieve the strong means of achieving the end of effective data protection regime.

The rights model also advocates that there would be prescribed set of rights that would be provided for everyone irrespective the consensual mechanism. It would stimulate the shifting of consequences of the harm to the fiduciaries in place of principals. The regime would also be mindful of the harm caused to the principals by violation of their data rights and the liability that the data fiduciary would have to carry.[134] These foundations of rights model

[133] Takshashila Discussion Document, Beyond Consent- A New Paradigm For Data Protection https://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf

[134] Founding Fuel, The Future of Privacy: A Conversation with Rahul Matthan, https://www.foundingfuel.com/article/the-future-of-privacy-a-conversation-with-rahul-matthan/

would make the legal framework of data protection strong and would allow the data principals to accept the legal norms and regime better.

With multiple organizations, radical changes in the way data is transacted, it is essential to bring in model that proves to be self-sustaining. Mere consent model does not prove to be self-sustaining and hence there is an immediate need to relook into the same. There are numerous challenges arising in fulfilling the requirements of meaningful consent. Hence, there is strong need to look for alternatives and to therefore bring an appropriate balance between the right and consent-based regime.

6. Recommendations and Suggestions

Cambridge Analytica, Justice Puttaswamy case, inclusion of right to privacy under Art.21 of Constitution, need to unlock digital economy while protecting the data of the individuals have forced the nation to enact a comprehensive data protection framework. In that regard, with the Committee Report of Justice Srikrishna came the Personal Data Protection Bill, 2018. With the march of digital India, digital payments, e-commerce outgrowth, data protection has become a major concern. Further, cross-border flow of data has occupied the central position with the growing partnerships in trade, numerous bi/multilateral trade agreements to that effect in place.

The need to have a law is further strengthened by the fact that Countries around the world are working towards having an effective law. Therefore, it becomes essential for India to frame its own laws to ensure that the business continue to exist in the new verticals. To achieve the given end, revisiting the existing privacy and data protection regime is vital. Process of bringing a new regime should be fastened. While looking at horizontal laws for comparison,

considerate focus should be given to unique features, context of the nation to regulate privacy and data protection in India. Though the Bill is welcome, there is a requirement to fine-tune the same by addressing some inherent issues in the Bill considering Puttaswamy case and GDPR. Therefore, the policy paper provides for recommendations/ key takeaways that imply to act as a means to achieve the end of having a robust law of privacy and data protection in India.

List of recommendations/key takeaways are:

- Being the largest democracy in the world, it is essential to serve the citizens in a requisite and appropriate manner. Puttaswamy recognizes privacy as a legal right and GDPR acts a forerunner to bring about effective privacy and data protection laws in India.
- The Information Technology Act, 2000 read with the SPDI Rules has major shortcomings with rapid technological expansion including lack of coverage of new players involved in information transaction, the nature of information that gets protection and the narrow imposition on body corporate that excludes State in its ambit.
- While law is essential, it is important to bring about harmony in terms of liberty to obtain information for legitimate state purposes, to serve citizens to satisfy their wants and needs. However such liberty should be backed with proper consent. In cases of national security, collective good, data transfer within borders, commercial utilization of data, a strict legal outlook should be provided for.
- Prescription, adjudication and enforcement should be interdependent and be qualified with one another. Substantial effect must be tested in tune with minimum contacts, nature and level of interaction to resolve jurisdictional issues. Hence, there is a need

to deliberate and delineate clear criteria to use fairness as a parameter to address jurisdictional issues.

- The exemption of application of Indian laws with respect to the data processed outside follows a presumption that the data of the foreign national would be protected in their territory under their respective data protection laws. However, an area of concern is when there exists no data protection law in that other contracting state. Such instance would substantially affect cross-border flow of information and data. Such issues require efforts to be taken by the entity to ensure there exist adequate data protection laws in the other contracting state.
- The committee also recommends that personal data of persons present in India would be protected. Those present in India is a phrase of wide conjecture to anyone present in India, at an individual level, it be an Indian citizen or resident or not.
- Protection of data principals from harm while allowing the data economy innovate is the need of the hour. Therefore, a robust data protection law that responds to the demands and could tackle to the unique requirements of nation has to be adopted.
- While incremental innovation is encouraged, law has to remain supreme in acting against data misuse. It should ensure threat to data is viewed seriously and decisions of the judiciary is enforced within and outside the territory as and when required.
- With volumes of data being processed by consent obtained through incorporated clauses of standard form contracts, there is consent fatigue. The consent-based model, is therefore losing relevance. Therefore, right based model that takes action against the data fiduciary for breach of right of data principal is proposed for the new legislation.
- Express rights being provided to the data principals makes the Bill efficient. However, the wordings in the Bill makes the right more restrictive. The express restrictive rights

take away all the other rights that the data principal could have by implication. The Bill has to incorporate data retention period, right to object against automatic processing and has to include right to erasure in right to be forgotten.

- The right to confirmation to the principal is accompanied with the processing fee of the same to be paid to the fiduciary. This may create issues since the imposition of a fee may discourage the data principal from exercising their right or they may also be unable to pay the same. Therefore, flexibility may be adopted in this regard. Furthermore, in order to comply with the requests, proper care must be taken in assessing the identity of the individual requesting for such information, or protection of identity of such individuals who may seek such information. This has not been addressed in the report.
- The Bill provides for obligations to the data fiduciaries who are established in the nation. The extraterritorial application is also reflected with respect to data fiduciaries obligations when they offer goods or services or perform activities with the data principals within India. However, there is no clarity on how the DPA of India would proceed with claims of infringement against data fiduciaries located outside with no permanent establishment or fixed place of business in India.
- Significant data fiduciaries are separate class of data fiduciaries who would be involved in processing of high-risk data. They are mandated to appoint a data protection officer. Foreign significant data fiduciaries are required to appoint a data protection officer as per the Indian Laws. However, the Bill does not provide for conditions of independency of such appointed officers. Further, compliance requirement relating to same are required to be strengthened with the sensitivity involved in processing of such data.

- Parental consent should not be the only option to process children data. Other possible options are to be explored. Further, parental consent and guardian data fiduciaries are eligible to give consent for a child who is below 18 years. The question of whether the child on attaining majority have the right to withdraw the consent. It is therefore proposed that the consent of child on attaining majority should be ratified consent with an option of withdrawing the same.
- Age verification mechanisms coupled with parental consent for protecting children from harmful effects of data processing such as targeted advertising, tracking, etc have not been substantially laid down, as this suggestion itself may fall prey to its inherent weakness in enforcement.
- Where guardian data fiduciaries have certain obligations that data fiduciaries need not necessarily follow, there could be an inconsistency in efficiently protecting the rights of children. Furthermore, there is a lack of clarity in the report as to how processing needs to be done in the best interests of the child, and left to the courts of law to deliberate upon.
- Adequate protection must also be accorded to personal data transferred abroad in national interest. There needs to be more clarity given on the kinds of personal data that may justify such extended protection or who may authorize such justification, but the committee is unable to reflect that in the report.
- Data mirroring and data localization have subjected the Bill into numerous debates. The Bill has a restrictive approach relating to cross-border transfer of data. It is proposed for the purpose of data mirroring, personal data should be considered major set within which would fall the identifiable personal data, within which would come the sensitive personal data which requires due protection and obligation from the data fiduciaries.

- The sub-set of the larger personal data that requires highest standard of protection is the critical personal data that should at any cost and compliance not be permitted to be transferred outside the nation. To the extent of critical personal data, the nation would have data sovereignty which should not be called in question. Considering such wider encompass, it is pertinent to define what a critical personal data is and what would be safety standards adopted by the nation to ensure that the data is duly protected.
- Regarding anonymized data, the provisions of the Bill contain safeguards and protection measures in cases where direct identification is possible. However, it is essential to include within its scope, indirect identification of personal that could be traced back to them. There is a need to reconsider and include indirect identification and requirement of anonymization of such indirect identification.
- There could arise a conflict of law situation regarding jurisdiction, which is another issue that needs to be resolved. However, the committee feels that there are more benefits if data is locally stored. This may not stand true for all kinds of personal data, therefore there needs to proper limitation on types of data that could be localized, while what may be allowed cross-border transfer – in order for India to take a middle path.
- Data breach that do not result in significant harm to the data principals and that which is a single failure due to technical error, force majeure should be classified as technical data breach and should be treated differently as compared to intentional data breach.
- Distinguishing intentional data breach and technical data breach is essential to impose penalties on entities in view of easing business transaction in the nation. Stringent penalties as under the Bill should not be imposed in case where the data fiduciary has not obtained any financial gain or has not obtained any unjust enrichment.

- Data breach by government departments finds a mere passing reference and has not been sufficiently addressed. Given the situation where the departments involved in data collection and processing have no turnover per se, their liability and penalty require further clarification.
- A separate board called the Data Protection Board is required to oversee the activities of DPA. The Board should also contain provisions which has the effect of reducing the overall burden imposed on the DPA.
- There is an immediate need to re-look into the appointments into the regulatory body, since cases relating to government being data fiduciaries would lead to unfavourable results where appointments are done by the Central Government directly.
- By invoking product liability, there is a high chance of dis-incentivization as the e-commerce companies acting as data fiduciaries may not be ready to bear the burden of product liability when consent is what was sought to be obtained from the said contract. However, it also serves to be an efficient mode as there is a linkage between defects between traditional products and an e-contract which might cause harm to the data principal due to data fiduciary's non-adherence to terms of the notice.
- Costs is a major factor that has to be taken care in Indian data protection framework. To reduce costs, the legislation could adopt purpose and use limitation of data. Focus on the size of the enterprise, their logistic combined with resource capacity in processing and storage of data with proper notice period to proceed against non-compliance would help reduce costs to enterprises.
- In cross-border transfer of data, adequacy and comparable protection has to be done on case to case basis. However, Sec. 41 (2) of the Personal Data Protection Bill, 2018 has to be suitably amended to set criteria on which the adequacy standards are to determined.

- There is a growing to bring an international treaty on privacy and data protection considering the growing gaps in the way national legislations provide for data protection. Further, to harmonize the international issues of free flow of data, enactment of a multinational framework which would enhance cooperation, unify laws and maintain international compatibility is encouraged.
- Data literacy does not merely mean educating and creating public of the positives and negatives of data processing. In essence, the data principal should be able to clearly understand the terms that he has agreed upon and should be provided with an option of opt-out from provisions that he does not wish to abide with.
- The Bill after its passage into Act provides twelve-month time period to data fiduciaries and entities to ensure compliance with the Act. Though compliance is mandated, finding out whether actual implementation and compliance is carried with is a question of the hour. Where the data fiduciaries not comply with the Act, then the rights and processes afforded would not serve the actual purpose of legislation.