INFORMATIONAL PRIVACY: LEGAL INTROSPECTION IN INDIA

Payal Thaorey[*]

Abstract

The ambivalent attitude of the Supreme Court has not been consistent whether to recognised privacy as a right included under fundamental right to life and personal liberty. The evolution and development of right to privacy can be traced in series of judgments conveyed by the Supreme Court of India over the period of time. Recently, efforts have been made by the court to define the tenuous concept of privacy and to recognise privacy as a framework of rights which is applicable in both public and personal domains. The advent of technology has changed the medium of privacy and introduced us with new dimension of privacy *i.e.,* informational privacy. Every individual has information related to his/her in some form or the other in the cyberspace. This information is either in the custody of state or non-state actors and not with the individual. Thereby possibility and dangers related to the misuse and mishandling of information cannot be ignored. Hence, in this research paper an in-depth analysis will be made about mapping the interest implicated to right to privacy related to information and how it accommodates informational privacy. The paper will also discuss and deliberate on various issues and concerns related to informational privacy and then examination of set of laws related to informational privacy will be made in order to understand the existing range of protection given to informational privacy.

I Introduction

THE CONCEPT of 'Privacy' has been a matter of debate, discussions and deliberations since its inception. However, the recent Judgement delivered by the Supreme Court in the case of *Justice K.S. Puttaswamy (Retd)* v. *Union of India*[1] has gained more prominence to the concept of Privacy in India as it dealt with the issues related to aadhaar database. The aadhaar is a database containing intrinsic details of the citizens including their bio-metric

[*] Assistant Professor, PGTD of Law, RTM Nagpur University, Nagpur.

[1] *Justice K.S. Puttaswamy (Retd)* v. *Union of India* (2017) 10 SCC 1.

information.[2] This creates a provision for privacy related to the person's information *i.e.,* informational privacy. It was argued that the compulsory requirement of aadhaar for access to social welfare schemes violates the right to privacy of an individual. As Aadhaar includes bio-metric information and it is connected with bank accounts, permanent account number (PAN) *etc.*, there is every possible chance that the information collected and connected through Aadhaar may get misused and will eventually hamper the framework of interest associated with privacy of citizens.

II Concept of privacy

Privacy is a subjective concept which varies from person to person. It originates from the term *"Privatus"* which means separated from the rest of the world. Steven Lukes, in his article on 'The Meanings of "Individualism" explains that the concept of Privacy is evolved and developed through the perception of "Individualism".[3] Individualism is a moral stance, political philosophy, ideology or social outlook that stresses "the moral worth of the individual". The theory of individualism reflects that an individual is an independent entity because the creator has granted life to him/ her and thereby an individual can avail all the freedom including privacy. According to John Locke, privacy is intrinsic to the notion of freedom. As per Locke's views, "a person who operated within the confine of a social contract, but is free within the confines of those contracts"[4] and only in the state of war he can give this freedom. Privacy allows every individual to be left alone in a core which is sacrosanct. As discussed by Charles Warren and Louis D. Brandeis in the famous article, "The Right to Privacy", "Once a civilization has made a distinction between the 'outer' and the 'inner' man, between the life of the soul and the life of the body, between the spiritual and the material, between the sacred and the profane, between the realm of God and the realm of Caisar, between Church and state, between rights inherent and inalienable and rights that are in the power of government to give and take away, between public and private, between society and solitude, it becomes impossible to avoid the idea of privacy by whatever name it may be called- the idea of a private space in which man may become and remain himself"[5].

---

[2] R.Venkata Rao, Subha Rao (eds), "A Public Disclosure on Privacy – An Analysis of *Justice K.S. Puttaswamy* v. *UOI*" (NLSIU, Bangalore, 1/2018).

[3]Steven Lukes, "The Meanings of Individualism" 32 (1) *JHI*, 45-66(1971), *available at:* http://www.jstor.org/stable/2708324. (last visited on Jan. 1, 2020).

[4]Bishop, Philip Schuyler, "Three theories of individualism" (2007). (Unpublished Graduate Thesis, University of South Florida), *available at:* http://scholarcommons.usf.edu/etd/636 (last visited on Jan. 2, 2020)

[5]Samuel Warren, Louis Brandies, "The Right to Privacy" 4 *HLR* 193 (1890).

Privacy is a prerequisite for the enlargement and salvation of personhood. Jeffrey Reiman defined privacy as, "a recognition of one's ownership of his or her physical and mental reality and a moral right to his or her self-determination".[6] Privacy is the inner sanctum of a person or reservation of private space which is inviolable, but still somewhere it is conditioned by his/her relationship with the rest of the society. As these relationships always carry with them questions to autonomy and free choice of an individual. Further, the pressure of the state and non-state entities design aspects of social existence which force an individual to surrender his choices.[7]

Alan Westin identifies four characteristics of privacy *i.e.,* solitude, intimacy, anonymity, and reserve.[8] According to Westin, "Solitude is a physical separation from others. Intimacy is a close, relaxed, and frank relationship between two or more individuals that results from the seclusion of a pair or small group of individuals. Anonymity is the desire of individuals for times of public privacy. Lastly, reserve is the creation of a psychological barrier against unwanted intrusion; this creation of a psychological barrier requires others to respect an individual's need or desire to restrict communication of information concerning himself or herself". These characteristics of privacy are so fundamental in an individual's life that it becomes inalienable unless it is affecting the society adversely.

As Salmond has defined right as, "an interest and protected by a rule of right. It is any interest, respect for which is a duty and this disregard of which is a wrong".[9] Considering the meaning of right expressed by Salmond, right to privacy is every individual's interest and therefore it not only needs to be recognised but also needs to be protected from state's interference as well as from third parties. This can be discussed by explaining the nature and scope of right to privacy in three phases wherein part I will recognise the strands of right to privacy, part II will discuss the protection of right to privacy by state and part III will focus on from whom the right to privacy needs to be protected.

Contents of privacy

[6] Jeffery L. Johnson, "A Theory of the Nature and Value of Privacy", 6(3) *Public Affairs Quarterly* 271-288 (1992), *available at:* https://www.jstor.org/stable/40435812 (last visited on Dec. 15, 2019).
[7] Right to Privacy: It's Sanctity in India", *available at*: https://ctconline.org/wp-content/uploads/pdf/2019/seminar-presentation/essay/R-11.pdf (last visited on June 3, 2019).
[8] Leon A. Pastalan, "Privacy as a Behavioural Concept" 45(2) *Social Science* 94 (1970), *available at:* https://www.jstor.org/stable/41963409 (last visited on Dec. 15, 2019).
[9] "Concepts of Law", *available at:* https ://shodhganga.inflibnet.ac.in/bitstream/10603/71969/3/03_chapter%201.pdf (last visited on Nov. 6, 2019).

i. The first strand recognised for privacy is related to physical or spatial privacy (space- in particular). This spatial privacy is protecting individual's bodily privacy within a confined demographic or territorial zone like in his/ her Home. Privacy as inner sanctum of an individual is very well protected in this case. In other words, privacy as explained by Justice Cooley of USA as *"the right of a person to be let alone".*[10] For eg--the preservation of constitutional liberty is aptly applicable in such forms of privacy.

ii. The second content views privacy as principally concerned with choice, an individual's ability to make certain significant decisions without interference. This conception of privacy is less concerned by having spatial boundaries and more concerned with a person's freedom to make personal choices. Further it not only includes freedom of choices but also includes freedom to choose the medium through which these choices will be executed. For example- use of technology for availing freedom of speech and expression in effective manner.

iii. Finally, the third content of privacy deals with protection, preservation and the flow of personal information. The advanced technological development bears the potential of generating databases having information which is personal as well as public. More precisely, information privacy concerns an individual's control over the processing i.e., the acquisition, disclosure, and use of personal information. Technology allows monitoring and tracing of individual's activities and behavioural patterns at every facet of his daily routine even though he or she is left alone. This interference is directly or indirectly not favourable the pursuit of individual's right to privacy.

These contents of privacy signify the nature of right to privacy wherein on one hand within individual it is protected horizontally *i.e.,* by providing an individual a choice to do or not to do anything by using any medium whereas on the other an individual's right to privacy is protected against State as well as against third parties from interference i.e vertical protection.

In part II the discussion will be made on how the right to privacy is protected. The primary protection is provided under the Constitution of India under article 19, article 21 and article 25. Privacy as a right for the first time came under the judicial lens in *M.P. Sharma* v. *Satish Chandra,*[11] wherein the provision of search and seizure as provided under the Criminal Procedural Code, 1973 was challenged as fundamental rights of the petitioner under article 19

[10]*Supra* note 5.
[11]*M.P. Sharma* v. *Satish Chandra,* (1954) SCR 1077.

(1) (f)[12] and article 20 (3)[13] of the Indian Constitution. The court held that search and seizure does not infringe constitutional rights. The court further observed that, *"*if the Constituent Assembly thought it fit not to recognise fundamental right to Privacy, analogous to 4th Amendment of US Constitution, then we have no justification to import it".[14]

In *Kharak Singh* v. *State of Uttar Pradesh,*[15] the Regulation 236 of Chapter –XX of UP Police Regulation was challenged as violating article 19 (1) (d) and article 21. The court held that knocking on the door of the petitioner in the mid-night is violating his right to Personal Liberty under article 21 of the Constitution of India. Thus, in this case right to privacy with respect to home comes within the scope of article 21 but with respect to public place, there exist no such right.

The Constitution of India implicitly guarantees certain concern for individual autonomy though in parts. As stated by Justice Krishna Iyer in *Gobind* v. *State of M.P,*[16] "In the application of the Constitution our contemplation cannot only be of what has been but what may be". Further Justice Matthew said, "Privacy has multiple facets and a rule of caution must be followed while examining the claims on case to case basis." Of course, privacy primarily concerns the individuals. It therefore relates to and overlaps with the concept of liberty. Therefore, it can be said that right to privacy gets covered under article 21, article 19 as well as article 25.

The court has not only recognised the right to privacy but also identified its various facets precisely through *telephone tapping case,*[17] *X* v. *Hospital Z,*[18] *Selvi* v. *State of Karnataka,*[19] *NALSA* case[20] etc. Over the years through series of judgements, judiciary has shown an attentive inclusive approach in recognising, protecting and conserving the right to privacy as a part and parcel of fundamental right in the democratic state. In tune with the constitution of India, the concept of privacy has evolved and developed both horizontally as well as vertically. Horizontally (within individual) it has included sexual autonomy as part of privacy, whereas vertically (state and individual) it imposes an obligation on state to protect

[12]Art. 19 (1) (f) guaranteed to the Citizens of India a right to acquire, hold and dispose of property. This right was later on omitted in 1978.
[13]No person accused of any offence shall be compelled to be witness against himself.
[14]*M.P. Sharma* v. *Satish Chandra,* (1954) SCR 1077.
[15]*Kharak Singh* v. *State of Uttar Pradesh,* (1954) SCR 1077.
[16]*Gobind* v. *State of M.P.,* (1964) 1 SCR 332.
[17]*People's Union for Civil Liberties (PUCL)* v. *UOI,* AIR 1997 SC 568.
[18] *X* v. *Hospital Z,* (1998) 1 SCR 723.
[19]*Selvi* v. *State of Karnataka* (2010) 7 SCC 263.
[20]*National Legal Services Authority* v. *Union of India,* AIR 2014 SC 1863.

and conserve right to privacy of every citizen. On the basis of above discussion, it is clear that right to privacy is an integral part of right to life and personal liberty and other freedoms guaranteed in article 19 and 21 f the Constitution.

In part III discussion will be made on against whom the right to privacy is being protected. In *Bodhisattwa Gautam* v. *Subhra Chakraborty*, [21] it is held that, "fundamental rights protect individuals from any arbitrary actions taken by both, the state as well as any individual". The notion of fundamental rights, such as a right to privacy as part of right to life, not only indicates that the states should refrain itself from interfering into an individual's matters but also restricts any other individual from doing so. The law enforces the state to take necessary actions against any such interference. However, this privacy right is not absolute or uncontrolled and is subject to reasonable restrictions as necessary for the protection of general welfare.

In *Kharak Singh's* case it was held that, "the security of one's privacy against the arbitrary intrusion by state is basic to a free society". The Supreme Court in this case was of the view that:

> if the action of the State is found to infringe any of the freedoms guaranteed to the individual under the Constitution of India, then the individual is entitled to the relief of mandamus which he seeks to restrain the State from taking such action.

Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others irrespective of the medium on which it is preserved. In *Ram Jethmalani* v. *Union of India (UOI)*[22] it was held that: [23]

> Right to privacy is an integral part of right to life, a cherished constitutional value and it is important that human beings be allowed domains of freedom that are free of public scrutiny unless they act in an unlawful manner. State cannot compel citizens to reveal, or itself reveal any of their details to the public at large, either to receive benefits from the State or to facilitate investigations, and prosecutions of such individuals, unless the State itself has, through properly conducted investigations, within the four corners of constitutional permissibility.

[21] (1996) 1 SCC 490.
[22] *Ram Jethmalani* v. *Union of India* (2011) 1 SCC 711.
[23] *Ibid.*

Therefore, the state needs to be cautious while interfering with individuals' right to privacy, because if an individual does not wish to disclose his information then the state cannot compel him to disclose unless the state establish valid grounds for such disclosures. Forceful disclosure of information would be violation of right to privacy.

The right to privacy is protected against an individual also. Knight Bruce in *Prince Albert* v. *Strange*[24] upheld that a third party intrusion into one's privacy results in grave violation of right to privacy and hence implies need of legal protection to right to privacy.[25] When a citizens' fundamental right to privacy is breached by fellow citizens is destructive of social order. Hence, the right to privacy is protected not only against the state but also against third parties.

From the analysis of the above literature, the various ways of defining privacy are;

1. Privacy means non-interference both by state as well as non-state authorities.
2. Privacy gives limited accessibility to others, wherein the limited accessibility is inclusive of secrecy, solitude and anonymity.
3. Privacy gives control over personal information or personal data. Personal liberty is embraced in data/informational control.
4. Privacy lies exclusive in aspects of personal lives that are intimate and /or sensitive.

After discussing the recognition and protection of right to privacy now the researcher will move ahead to discuss the conceptual analysis of informational privacy.

III Informational privacy: Conceptual analysis

Informational privacy is an emerging phenomenon. With the advent of technology and internet, new dimensions are being added to the traditional notion of right to privacy like informational privacy or data privacy. Technology allows an individual to generate both personal and non-personal information about him in the cyberspace knowingly or unknowingly. According to IITF Principle of the Unites States, Information privacy is "an individual's claim to control the terms under which personal information *i.e.,* information identifiable to the individual is acquired, disclosed, and used".[26] The informational privacy (also referred as data privacy) does have the essence of privacy law which lies in the claim of

[24] *Prince Albert* v. *Strange,* [1849] 64 ER 293.
[25] Aishwarya C.R., "Privacy in Cyber Space- Concerns and Challenges" 3 *Bharti Law Review* 175 (2016).
[26] Principles for Providing and Using Personal Information ("IITF Principles") issued by the Clinton administration's Information Infrastructure Task.

an individual to control disclosures, use, or access to information pertaining to that person[27]. According to Westin, "the complete authority on the disposal of personal information lies with the individual as a part of his privacy right. He further says, Privacy as the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others".[28] This claim can be grounded in social policies or in constitutional precepts about individual autonomy.

Informational privacy or data privacy is the relationship between accumulation and dissemination of data, technology, legal and political issues surrounding them[29]. It covers information that links individual specifically with particular events, background facts, or other information. The Informational privacy rights depend on whether the subject matter consists of "personal information"[30] or non-personal information because every sort of non-personal information will not be able to claim right to privacy. Initially let's evaluate the term personal information and then the non-personal information.

Personal information

Here "Personal" does not mean especially sensitive.[31] Rather, it describes a relationship between the information and a person, namely that the information whether sensitive or trivial is somehow identifiable to an individual.

Personal information can include,

i) any information which creates an ownership relation to the individual,
ii) any descriptive relation to the individual and
iii) any instrumental mapping relation to the individual[32].

An individual owns his personal information which as per his/her interest he/she offers and describe to the society as a medium of identification. This information may include the individual's biometric state, such as sex, height, weight, blood type, fingerprint, retina pattern, DNA, or state of health. It may relate to biographical facts, such as birth date, marital

[27]Raymond T. Nimmer, *Information Law* (West Law, Minnesota, 1st edn. 2002).
[28]*Ibid.*
[29]"Information Privacy", *available at*: https://en.wikipedia.org/wiki/Information_privacy#cite_note-1 (last visited on Dec.10, 2019).
[30]U.S. Dept of Commerce, Privacy and the NII: Safeguarding telecommunications Related to Personal Information 2 (1995).
[31]This is an important clarification because usually personal privacy is referred and related to personal sensitive information only.
[32]Jerry Kang, "Information Privacy in Cyberspace Transactions" 50(4) *Stanford Law Review* 1193-1294 (1998), *available at:* https://www.jstor.org/stable/1229286 (last visited on Mar. 1, 2019).

status, sexual orientation, immigration status, criminal history, or educational degrees and also identify social connections, such as membership in religious and political organizations.

The descriptive information includes records which are more discrete wherein transient actions are taken by an individual.[33]For example, it contains information related to data footprints of individual visiting a particular store online at a particular time to purchase a particular item. Such information is regularly collected by undercover surveillance through cyberspace.

Finally, the information that is not provided by the above two categories but still can be personal if it is the information which is instrumentally mapped for the individual's institutional identification such as secured access, or provision of some services or goods.[34]Usually, such information bears no prior relation to the individual. The best example is the UIDAI.[35] In no way does the individual create or author Aadhaar number. Nor does it describe the individual's state-of-being or actions, except that it is mapped to the individual by the federal government for record keeping purposes. This category of personal information includes confidential[36] pieces of information that act as keys to secured function or processes, such as passwords to login to a network and to use automatic teller machines.

Non-personal information

If information is not related to an individual, then it is not personal information and, according to the definition of privacy it lacks privacy significance. This is because of three factors:[37]

> First, the information simply may not be about an individual human being. Therefore, it is not personal information, which means it has no privacy concerns.

Second, although about an individual, the information may not be identifiable to that specific individual because it has been anonymized.[38] For example, information filed by the individual in the questionnaire or responses, views, opinions expressed in it, will be considered as information given by individual but it is anonymous hence no privacy threat.

---

[33]*Ibid.*
[34]*Ibid.*
[35]Unique Identification Authority of India.
[36]Confidentiality is often mistaken for privacy. The former as a measure of the degree and terms of disclosure. If information has been disclosed to many people or to the world large, then it is said to be "not confidential".
[37]*Supra* note 32.
[38]*Ibid.*

Third, although about individuals and not anonymized, the information directly identifiable to a group and only indirectly identifiable to the individuals constituting that group. Under one interpretation of the privacy definition, because the information is directly about the group and not about the individuals that constitute the group, the data is not personal and stand outside privacy realm. But this seems formalistic. As the information is regarding the group and it applies to all the members of the group, it means that it is applicable to all the individuals and hence it becomes personal information of that individual.[39]

The researcher feels that, what we understand as "personal" depends on the nature of information. For example, a corporation has privacy interests. A corporate being a legal person,[40] does have its own identity but at the same time it has to also maintain the identity of the individuals who make up the corporation. This means that the corporate does have its own privacy at the same time it is also bound by the privacy of the individuals working in it. Hence, the data related to the tax payment by the individuals as employee of the company or stakeholders of the company is the matter of privacy for the company, which the company neither use nor disclose without the permission of the individual.

The idea of informational privacy stems from the concept of privacy which is discussed earlier. The broader view of informational privacy is applicable to both personal information as well as group information. Informational privacy can be understood as proposed by Westin, "the right to control the way others use the information concerning us" becomes part and parcel of right to privacy. Therefore, informational privacy provides framework of rights which is inclusive of rights related to both personal as well as public domains.

Indeed, collection of sensitive data and social and individual profiling may give rise to discrimination; privacy is therefore to be regarded as "the protection of life choices against any form of public control and social stigma"[41]. Since the information flow do not simply contain "outbound data" (to be kept off others' hand) but also "inbound" information on which one might wish to exercise a "right to know",[42],allows informational privacy as part of privacy. This ultimately emphasise on the data privacy *i.e.,* "the right to keep control over one's information and determine the manner of building up one's own private sphere".

[39]*Ibid.*
[40]*Salomon* v. *Salomon & Co Ltd,* [1896] UKHL 1AC 22.
[41]Serge Gutwirth, Yves Poullet, *et. al., Reinventing Data Protection?* Springer, 2009.
[42]*Ibid.*

IV Technology and informational privacy

Under the regime of privacy rights, every individual wants to keep his or her personal affairs to himself, but in the electronic transactions, variety of individual's information are collected and stored, which can easily make others to identify that individual.[43] Technology enhances productivity and provides opportunities, livelihood, recognition and social growth. It can be said that an individual's autonomy in the information society can be recognised as an "informational self-determination".

In *Puttaswamy* v. *Union of India,*[44] Justice Nariman stated "we can ground physical privacy in article 19 (1) (d) and (e) read with article 21; privacy of choice in articles 19 (1) (a) to (c), 20 (3), 21, and 25 and ground personal informational privacy under article 21".[45] He was of the view that, "the core value of the nation being democratic, for example would be hollow unless persons in a democracy are able to develop fully in order to make informed choices for themselves which affect their daily lives and their choice of they are governed".[46] Thereby an individual has the right to make his choices which is intrusive of allowing him to use any medium to express his views like print medium, digital platforms, social media etc but while an individual is availing his right of making choices an equally opposite duty lies on the state to take care that such right to choose should not get affected. What an individual is choosing is an absolute matter of his privacy and the state cannot have a hold on individuals' choices. Any information or database which is generated by executing these freedoms assigned to an individual can become his/her property unless provided by law.

Taking reference from *Puttaswamy's* judgment, the Supreme Court in *Indian Hotel and Restaurant Association (AHAR)* v. *The State of Maharashtra,*[47] considered the data stored in CCTV footage is the personal information of the person. The court held that, "complete surveillance of activities through CCTV cameras inside the premises of dance bars is excessive and disproportionate. The monitoring, recording, storage and retention of dance performances causes unwarranted invasion of privacy and would even subject women bar dancers to threat and blackmail". As the CCTV footage provides strong source for identifying an individual it becomes part of his information which attracts right to privacy.

[43]Gargi Rajvanshi, Mayank Singhal, "Data Privacy Law and Growth of E-Commerce: An Indian Perspective" 2 *Bharti Law Review* 9 (2016).
[44]*Puttaswamy* v. *Union of India* (2017) 10 SCC 1.
[45]*Supra* note 1.
[46]Per Nariman J. at Para 81, *Puttaswamy* v. *UOI* (2017) 10 SCC 1.
[47]*Indian Hotel and Restaurant Association (AHAR)* v. *The State of Maharashtra* (2019) 1 SCC 45.

The recent admission by Facebook that, "the data of 87 million users, including 5 lakh Indian users, was shared with Cambridge Analytica through a third-party application that extracted personal data of Facebook users who had downloaded the application as well as their friends, is demonstrative that users did not have effective control over data".[48] As per the recent statistics there are 326.1 million social media users in India, out of which 260 Million are Facebook users till April 2019. The statista.com has predicted that India will have 448 million social media user by 2023.[49] These 326.1 million media users share online photo, status update, Twitter post and blog entry by and about them which will be stored forever. These figures show that abundant personal data of Indian Citizens is available on the internet on which these users have absolutely no control.

Technology has the capability to generate extremely big data sets that may be analysed computationally to reveal patterns, trends, and associations, especially relating to human behaviour and interactions across globe. As per the report of the committee on a Free and Fair Digital Economy Protecting Privacy, Empowering Indians, "Data gathering practices are usually opaque, mired in complex privacy forms that are unintelligible, thus leading to practices that users have little control over. Inadequate information on data flows causing tangible harms are unfortunate reality now".[50] The Internet has brought new concerns about privacy in an age where computers can permanently store records of everything. In India under the Aadhaar Card Act, through UIDAI the Government is authorized to collect, use, transfer, store and processing of both biometric as well as demographic data of the citizens, wherein the citizens absolutely don't have any control of this data.

Justice Chandrachud in *Puttaswamy's* case was of the view that, "We are in an information age. With the growth and development of technology, more information is now easily available. The information explosion has manifold advantages but also some disadvantages. The access to information, which an individual may not want to give, needs the protection of privacy".[51]

Technology on one hand is expanding the scope of right to privacy by including personal information as a part of privacy, whereas on the other it has reduced the scope for control of

[48]Union Ministry of Electronics & Information Technology, Government of India, "Report: Committee on A Free and Fair Digital Economy Protecting Privacy, Empowering Indians" (2017).
[49]*Available at:* www.statista.com (last visited on Dec 10 , 2019).
[50]*Supra* note 48.
[51]Per D.Y. Chandrachud J. at para 457, *Puttaswamy* v. *UOI* (2017) 10 SCC 1.

individual over it and extend the control of private parties on such information. Presently, the personal data is controlled by both state as well as non-state organisations like facebook, twitter etc. To make the situation worse, the competition in today's world has compelled the business structure to use this 'personal data' to design their business strategies to earn economic benefits. Thus, this personal information of an individual may be misused commercially, socially, politically, economically, religiously not only by the state but also by the non-state actors as well. Therefore, it is more essential that this data should be regulated and protected irrespective of the fact whether it is controlled by state or non-state organisations so that individual's right to informational privacy would not be affected.

V Informational privacy – Issues and concerns

Puttaswamy case is a landmark judgment in many respects but significantly it has emphasized the issue of recognising and protecting informational privacy in India. It was held that, "to make this right meaningful, it is the duty of the state to put in place a data protection framework which, while protecting citizens from dangers to informational privacy originating from state and non-state actors, serves the common good. It is this understanding of the state's duty that the committee must work with while creating a data protection framework".[52] Undoubtedly the views of the judiciary are progressive towards accommodating informational privacy as a part of privacy, the researcher expresses her concern that these views may open up a new floodgate for litigation on some pretext or the other related to right to privacy. Apart from the primary concern about individuals having no control over information about them and their information is used for trade related purposes there are some other additional concerns which are discussed below:

No control over information

The RTI query on UIDAI revealed that the terms of contract of UIDAI with US-Based biometric service providers like L-1 Identity Solutions Operating Company Private Ltd, Morpho and Accenture Services Private Ltd used the aadhar data. This is apparent from contracts' clause 15.1, on 'Data and Hardware', as well as clause 3, which authorizes the collection, use, transfer, storage and processing of data.[53] The burning question here is 'Do individuals have control over the manner in which information pertaining to them is accessed

[52]*Supra* note 48.

[53]Data Security and Breach of Privacy, 2017, *available at:* https://www.dailypioneer.com/2017/columnists/aadhaar-data-security-and-breach-of-privacy.html (last visited on Jan. 8, 2020).

and processed by others?'[54] Therefore, the Supreme Court has opened the opportunity for the citizens to appeal against the government under certain established principles concerning these constitutional rights which can protect the informational privacy.

Absence of right to be deleted

Considering the potential of social media and World Wide Web, Justice Kaul identifies the need for "right to be forgotten".[55] He was of the view that, "the right to be forgotten refers to the ability of individuals to limit, de-link, delete, or correct the disclosure of personal information on the internet that is misleading, embarrassing, irrelevant, or anachronistic".[56] Due to right to privacy an individual must have control over his personal information, which means if he wishes to delete his information then it must get erased from the cyberspace However, the data protection laws across world supports right to be forgotten but not right to be deleted. Forgotten means that the data will be there in cyberspace, only thing is it will appear at the end of search pages whereas right to be deleted gives control to the owner of information to delete it permanently from cyberspace.

Lack of cross border protection

An interesting diagnosis made in *Puttaswamy* is the possibility of enforcing fundamental right not only against state action, but also against private individuals. As theorised by Justice Chandrachud, for keeping the data privacy notion alive, the data can be regulated by the state through the formulation of an appropriate data protection law which may include regulation of data misuse by the private individuals also. So far the protection of right to privacy within domestic jurisdiction against state and non-state actors is thoroughly discussed and regulated by the Indian judiciary and law making bodies. But cross border protection of informational privacy is still unregulated.

Absence of informed consent

Another threat identified by judges in informational privacy is absence of informed consent. In the present era of 'click-wrap' contracts, most privacy policies are highly convoluted and

[54] *Supra* note 2.
[55]Per Kaul at Para 64, *Puttaswamy* v. *UOI* (2017) 10 SCC 1.
[56]Government of India, Report: *Committee on A Free and Fair Digital Economy Protecting Privacy, Empowering Indians* (Union Ministry of Electronics & Information Technology, 2017).

couched in legalese.[57] In reality, hardly anyone reads the consent document on the internet. This absolute nature of acceptance or denial and the indispensable nature of most digital services raises pertinent challenges to the traditional understanding of "informed consent", in so far as whether people who are unaware of usage and repercussions can give consent to use of the same. The judges showed their concern about regulation of informational privacy, as they feel that the consent should not be restricted only for data collection but also should be extended for the purposes for which it has been collected and to the extent it was disclosed.

As the data flow is loosely regulated in India, it poses a difficulty to any security related mechanisms. In every information Privacy violation, remedy is sought from other peripheral legislation as the Data Protection Bill, 2019 is still in the making. These peripheral laws are discussed below:

VI Informational privacy: Legal Introspection in India

In India currently we shuttle the word 'informational privacy' with 'data privacy' as no legal definition is available so far. The researcher wants to make it clear that the non-availability of definition of Informational privacy doesn't reduce the intensity of understanding the dangers related to protection of informational privacy or data privacy. The technological developments are uncontrollable but certainly states can make an effort to regulate it through law. As a regulator of both social life and individual behavior through its distinct institutions and practices, law cannot afford to be dormant or static on any issue prevailing in the society. Informational privacy though being an emerging phenomenon, law cannot be keep it unregulated. Efforts have to be made to enact laws which can carefully deal with it.

As the Data Protection Bill, 2019 is pending with the Parliament, India does not have a comprehensive legislative framework to deal with data privacy. So the evaluation of other peripheral laws will help in understanding the nature of regulation of informational privacy. Some of those are discussed below:

The Indian Telegraph Act, 1885

Early reference of protection of information can be traced way back in 1885 under the Indian Telegraph Act, 1885 wherein under section 5 (1) temporary possession of the message by the authority is permitted and under section 5 (2) the interception of messages by the authority is

[57] *Supra* note 2.

permitted only in case of any public emergency or in the interest of public safety.[58] Thereby, state will interfere with information communicated in the form of message only in case of any public emergency or in the interest of public safety and in any other case the state cannot interfere, which is nothing but the protection of right to privacy over the message. Further section 24 provides for the consequences of attempting to learn the contents of messages unlawfully. Any unlawful access to message is a punishable offence, therefore the privacy in message was protected under this act.

The Information Technology Act, 2000

To counter the challenge of data privacy, another significant reference can be taken from the Information Technology Act, 2000. An amendment was made in the IT Act in 2008 by adding section 43A and section 72A for dealing with sensitive personal data. Section 43A is creates a private right of action in civil law by which any person can sue a body corporate for negligent handling of its sensitive personal data or information.

- Body corporate possessing, dealing, or handling, any SPD[59] or information in a computer resource.
- Then, the body corporate has a duty to implement and maintain reasonable security practices.
- Causing wrongful gain or wrongful loss to any person
- The body corporate shall be liable to pay compensation.[60]

[58] The Indian Telegraph Act, 1885. S. 5. Power for Government to take possession of licensed telegraphs and to order interception of messages.
On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a state government or any officer specially authorized in this behalf by the Central Government or a state government may, if satisfied that it is necessary or expedient so to do, take temporary possession (for so long as the public emergency exists or the interest of the public safety requires the taking of such action) of any telegraph established, maintained or worked by any person licensed under this Act.
On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a state government or any officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order:
Provided that press messages intended to be published in India of correspondents accredited to the Central government or a state government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section.
[59]Sensitive Personal Data.
[60]*Supra* note 25.

Section 72 of the act deals with breach of confidentiality and privacy. Anyone who secures access to electronic records of the other without of the consent shall be liable for violation of right to privacy of the other person. This section has been criticized for being inadequate as it applied only to the statutory authorities exercising their power under the Act. In 2008 amendment, section 72A has been inserted, now the position is it applies to any person handling data under a contract, including but not limited to network service providers. Hence the IT Act, 2008 holds the data privacy law against the state as well as third parties.

The Information Technology (Reasonable Security Practices and Procedures and sensitive personal information) Rules, 2011:

Under this rule 4 require body corporates holding sensitive personal information of users to have a privacy policy for handling such information under lawful contract. Rule 5 lays down the security standards and procedures to be followed for collecting the information from the user. This must include consent and lawful purpose for collecting SPD.[61] Rule 5 D states that the body corporate cannot retain that information for longer than is required for the purpose. Rule 6 provides that, disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information. Thus, it can be said that the IT Rule, 2011 protects the sensitive personal information from unlawful disclosures. This means the privacy of the information must be protected by the body corporates.

Regulatory bodies

Clause 37, 39 of the Unified Access Service License and clause 42 of the Cellular Mobile Telephone Service License require the licensee, *i.e.,* the telecommunication provider to adhere to certain confidentiality conditions with respect to customer information to ensure protection of privacy of communication and to ensure that unauthorised interception of message does not take place.[62] Clause 21 of the national long distance license requires the

[61]The term "sensitive personal data or information" of a person is defined to mean such personal information which consists of information relating to— (i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise: provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these regulations.

[62]Data Protection and Privacy Issues in India, 2017, *available at*: https://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf (last visited on Dec.15, 2019).

licensee*, i.e.,* the telecommunication provider to adhere to certain confidentiality conditions with respect to customer information.

The Aadhaar Act, 2016

After the implementation of Aadhaar Act, one of the major worries is whether collecting and compiling the demographic and biometric data of the residents of the country to be used for various purposes is in breach of the fundamental right to privacy? The answer to this question is discussed below:

The Government of India through The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 has recently mandated the use of the biometric database known as aadhaar card to deliver targeted subsidies, benefits and services. The biometric information of every individual is unique and this uniqueness makes the individual "only one in the world". Thus the biometric information is extremely sensitive and personal in nature and attract right to privacy which needs to be protected.

Section 28 of the act provides that the UIDAI shall ensure the security of identity information and authentication records of individuals. Section 29 prohibits the sharing of core biometric information[63] collected or created under the Aadhaar Act, with anyone for any reason; or be used for any purpose other than generation of Aadhaar numbers and authentication under the Aadhaar Act. Also, under the Aadhaar (Sharing of Information) Regulations, 2016 sharing of core biometric information by the authority is prohibited.

However, the Act is silent regarding consent being acquired in case of the enrolling agency or registrars. Section 8 provides that any requesting entity will take consent from the individual before collecting his/her Aadhaar information for authentication purposes, though it does not specify the nature (written/through fax).[64] On one hand Aadhaar is mandatory for every individual for getting benefits, whereas on the other the mode of getting consent for Aadhaar is unclear. This may affect the informational privacy of the individual enrolling for Aadhaar.

Further whenever an individual desire to avail the benefits linked with Aadhaar, he needs to provide Aadhaar details including core biometric information to various agencies assigned by

[63]The term "core biometric information" has been defined to mean finger print, iris scan, or such other biological attributes of an individual as may be specified by regulations.
[64]*Available at:* https://cis-india.org/internet-governance/blog/aadhaar-act-and-its-non-compliance-with-data-protection-law-in-india (last visited on Dec. 17, 2019).

the state like banks but are not state dealing with distribution of benefit/subsidy. Therefore, the individual left with no choice but to share his Aadhaar details on terms and conditions prescribed by those non-state agencies which in a way is violation of informational privacy. The Aadhaar Act creates biggest paradox for the right to informational privacy as in order to get benefits linked with Aadhaar, an individual need to surrender his biometric information which is part of his right to privacy.

Eventually the Union government constituted a Committee chaired by Justice B.N. Srikrishna, former judge of Supreme Court, for preparing report on A Free and Fair Digital Economy Protecting Privacy, Empowering Indians. The committee released its report and proposed Draft Personal Data Protection Bill in July, 2018.

Here it is essential to understand that all these laws neither address nor respond to the issues raised by researcher in the earlier section. Therefore, the need for comprehensive law on data privacy prevails. Recently in May 2018, the European Union has adopted General Data Protection Regulation which replaced the earlier EU Directive 95/46/EC for processing and protecting personal data within EU and outside EU if the processed data is related to EU in any way. The GDPR has strengthened the conditions for consent from the owner of information. Also, penal provisions are inserted in it so as to strictly deal with informational privacy violations. This is indeed a good initiative taken by EU to deal with protection of data. Indian law making bodies must take reference from GDPR while enacting laws for regulating data privacy.

VII Conclusion

After introspecting the above discussion about informational privacy, it appears that the right to life and liberty guaranteed under article 21 of Indian Constitution which protects an individual against both state and non-state actors can very well accommodate informational privacy. The advancement in technology helps in generating databases related to individuals, wherein ideally it is the individual who should be in-charge of it, but unfortunately he is not. The presence of technology helps to make information about an individual's private life available to others and tends to influence and even to injure the very core of an individual's personality *i.e.,* his informational privacy.

The current Indian regulatory framework on informational privacy and data protection is not sufficiently adequate to address the growing concerns arising on account of collection,

leaking and linking of data. Certainly there is a need for comprehensive legislation which can deal with informational privacy and its related issues. Once the Data Protection bill, 2019 gets enacted, we can expect that the informational privacy will be regulated carefully in the coming future. As the technology grows at an unimaginable speed, further research on concerns related to protection and regulation of informational privacy is certainly the need of an hour.