Journal Articles ISSN:2582-1903 *Shimla Law Review*

2018

CONTOURS OF RIGHT TO PRIVACY IN THE INFORMATION AGE: SOME RANDOM REFLECTIONS ON THE *PUTTASWAMY* JUDGMENT

Meena S. Panicker

DOI: https://doi.org/10.70556/hpnlu-slr-v1-I1-2018-07

Contents

Volume I 2018 Shimla Law Review

Contours of Right to Privacy in the Information Age: Some Random Reflections on the *Puttaswamy*[*] Judgment

Introduction

The Government of India's decision to link Aadhaar with various welfare schemes made imperative the linking of Aadhaar details with PAN/mobile number/bank account/income tax etc. This decision re-augmented the discussion on the right to privacy within circles including the apex court. Twenty-seven writ petitions were filed at various points of time challenging the constitutionality of the Government decision. The petitions contended that right to privacy is incorporated in Part III of the Constitution of India and therefore, the mandatory submission of Aadhaar details will directly hit the right to privacy of the individual. A three judges bench of the Supreme Court passed an order whereby the matter was referred to the constitution bench.[1] The

---

[*] *Justice K.S. Puttaswamy* v. *Union of India*, (judgement delivered on 24 Aug., 2017). *Available at*: http://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf. (last visited 07 Apr., 2018).

[1] A three judge bench of the Supreme Court in its order in *K.S. Puttaswamy* v. *Union Of India* (WPC No. 494 of 2012) dated 11 August 2015, referred the issue to be decided by an appropriate Bench, in following terms: "[W]e are of the opinion that the cases on hand raise far reaching questions of importance involving interpretation of the Constitution. What is at stake is the amplitude of the fundamental rights including that precious and inalienable right under Article 21. If the observations made in *M.P. Sharma* (supra) and *Kharak Singh* (supra) are to be read literally and accepted as the law of this country, the fundamental rights guaranteed under the Constitution of India and more particularly right to liberty under Article 21 would be denuded of vigour and vitality. At the same time, we are also of the opinion that the institutional integrity and judicial discipline require that pronouncement made by larger Benches of this Court cannot be ignored by the smaller Benches without appropriately explaining the reasons for not following the pronouncements made by such larger Benches. With due respect to all the learned Judges who rendered the subsequent judgments—where right to privacy is asserted or referred to their Lordships concern for the liberty of human beings, we are of the humble opinion that there appears to be certain amount of apparent unresolved contradiction in the law declared by this Court… . Therefore, in our opinion to give a quietus to the kind of controversy raised in this batch of cases once for all, it is better that the ratio decidendi of *M.P. Sharma* (supra) and *Kharak Singh* (supra) is scrutinized and the jurisprudential correctness of the subsequent decisions of this Court where the right to privacy is either asserted or referred be examined and authoritatively decided by a Bench of appropriate strength."
The reference came to be decided in *Justice K.S. Puttaswamy* v. *Union of India*, (WPC No. 494 of 2012, judgement delivered on 24 Aug., 2017). *Available at*:

Constitution bench then stated that the matter requires an examination by a larger bench and therefore, referred the matter to a nine-judge bench.[2] This bench delivered a judgment upholding the right to privacy as part of Constitution of India.[3]

While delivering the judgment, the Court conducted a detailed examination of the prominent previous decisions of the Court and overruled two of them.[4] Apart from this, the Court examined the contours of right to privacy in an era of information technology. The present paper focusses upon the appropriateness of the Supreme Court's decision on the latter part, in view of the fact that, the digital era raises serious questions on credibility of data protection. The Court in this case held that privacy concerns are a serious issue in the age of information.

The paper is divided into the following parts: following the introduction in Part I, Part II delves into the expanding horizons of internet uses leaving little option or at times no discretion with the individual. Internet services and their usage by individuals may have consequences in terms of intrusion into right to privacy. This intrusion may be caused by the state or non-state entities. Part III therefore, examines the extent of privacy right maintainable by the individual and the compelling state necessity which mandates access to data of the individual. The Court fixed right to privacy within Article 21 and Part IV examines the requirements of due process for intervention with the right to privacy. The admitted position of the Court is that in the age of information, the state requires data for some legitimate purposes which would then make the state accountable for a fool proof data protection law. Part V examines this balancing act of the Court.

Internet Services, the Kind of Uses and Consequences

Privacy debate engulfed unassuming proportions with the ever expanding nature of information technology and internet services and usage. An array of instances is narrated by the Court wherein the individual shares data with the service providers. As the Court observes:[5]

> … Individuals connect with others and use the internet as a means of communication. The internet is used to carry on business and to buy goods and services. Individuals browse the web in search of information, to send e-mails, use instant messaging services and to download movies. Online purchases have become an efficient substitute for the daily visit to the neighbouring store. Online banking has redefined relationships between bankers and customers.

---

http://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf. (last visited 07 Apr., 2018). (Hereinafter referred as 'privacy judgment').

2 *Supra* ('privacy judgment') note 1, at para 2, (Opinion of Nariman J).

3 *Id*.

4 *M.P. Sharma and Others* v. *Satish Chandra, District Magistrate, Delhi, and Others*, 1954 SCR 1077; and *Kharak Singh* v. *State of U.P.*, (1964) 1 SCR 332. The first case was decided by 8 judges and second case was decided by 6 judges.

5 *Supra* ('privacy judgment') note 1, at para 170 (Opinion of Dhananjay Chandrachud J).

> Online trading has created a new platform for the market in securities. Online music has refashioned the radio. Online books have opened up a new universe for the bibliophile. The old-fashioned travel agent has been rendered redundant by web portals which provide everything from restaurants to rest houses, airline tickets to art galleries, museum tickets to music shows.

However, what is the option left for the individual requires to be debated. An individual may open an e-mail account innocuously just for facilitating her communication with relatives, friends, office etc. What shall be the credibility of the data she entered while opening the e-mail account? Where is it stated that her data requires to be authentic for opening an e-mail account or the service provider will verify the credibility of her data. Over the years, internet based activity expanded from mere e-mail usage to a wide variety of uses like banking transactions, online purchases, online business, beneficiary to state welfare schemes etc. This expansion in internet based uses slowly demanded authentic details from the user indirectly.

Access to internet leaves electronic tracking without the knowledge of the user and profiles her food habits, language, health, hobbies, sexual preferences, friendships, ways of dress and political affiliation[6]. The electronic tracking makes it possible to assess the nature of her personality. This description about electronic tracking gives an account of the kind of intrusion into the sphere of privacy of the user. The electronic tracking submits involuntarily oneself to the nuances of technology based services wherein the role of the user is nil or at the mot minimum.

The Court further observes the following to explain the nature and unlimited extent of invasion of privacy through internet usage:[7]

> Popular websites install cookie files by the user's browser. Cookies can tag browsers for unique identified numbers, which allow them to recognise rapid users and secure information about online behaviour. Information, especially the browsing history of a user is utilised to create user profiles. The use of algorithms allows the creation of profiles about internet users. Automated content analysis of e-mails allows for reading of user e-mails. An e-mail can be analysed to deduce user interests and to target suitable advertisements to a user on the site of the window. The books which an individual purchases on-line provide footprints for targeted advertising of the same genre. Whether an airline ticket has been purchased on economy or business class, provides vital information about employment profile or spending capacity. Taxi rides booked on-line to shopping malls provide a profile of customer preferences. A woman who purchases pregnancy related medicines on-line would be in line to receive advertisements for baby products. Lives are open to electronic scrutiny. To put it mildly, privacy concerns are seriously an issue in the age of information.

---

[6] *Id.*

[7] *Id.*, at para.171.

As of December 31, 2016, India has 1151.78 million telecom subscribers out of which 683.14 million are urban subscribers.[8] The internet subscribers are 391.50 million out of which 236.09 million are broadband subscribers and the remaining are wireless subscribers.[9] 30.56 per 100 people are internet subscribers. 68.86 per 100 people in urban India are internet subscribers.[10] This figure in rural India is 13.08.[11] The Court relied on this data to assess the gravity of the privacy issue. No longer a divide exists between urban and rural India at least in the context of internet users though the percentage may vary. The subscription-wise varied percentages between urban and rural India do not hinder people's desire to have an internet account/subscription. The mushrooming growth of internet café/computer learning centres replace the type writers/type learning institutes of the earlier era. The Government has adopted measures to move their activities to the e-governance model. Today, the payment for many basic utility services like electricity can be done online. This desire for e-governance both at the government level and people's level exist despite constraints in various forms.

Individual's Privacy and Data Necessity (Compelling Necessity) by the State

As Part II explained the ambit and scope of internet usage and preferences/options for the users, questions are posed about the protection of privacy of users. As the internet uses are for varied purposes, privacy as a matter of fact cannot be claimed on every usage. There are some spheres of usage of information about an individual where a reasonable expectation about right to privacy exists. The Court discusses three categories of information, namely, non-rivalrous, invisible and recombinant.[12] Non-rivalrous nature of information makes its simultaneous usage by many people.[13] It may be invisible because data based on the information may be stored, accessed and disseminated without notice[14]. It has recombinant value as the output data can be used as an input for generating more data output.[15]

The Court/institution/state may not be able to conceive of the possible uses of information/data and its consequences. The information may be used for monitoring the actions of the individual. Big databases are generated based on the activities and

---

8 Press Release 45/2017, *available at:* http://trai.gov.in/sites/default/files/PR_No.45of2017.pdf , quoted in *Supra* ('privacy judgment') note 1, at para 172 (Opinion of Dhananjay Chandrachud J.).

9 *Id.*

10 *Id*.

11 *Id.*

12 *Supra* ('privacy judgment') note 1, at para 173 (Opinion of Dhananjay Chandrachud J).

13 *Id.*

14 *Id.*

15 *Id.*

engagement of the individual with internet. These concerns are expressed by the Court through the reproduction of the following thus:[16]

Yvonne McDermott speaks about the quantified self in eloquent terms:

> "…The rise in the so-called 'quantified self', or the self-tracking of biological, environmental, physical, or behavioural information through tracking devices, Internet-of-things devices, social network data and other means (Swan. 2013) may result in information being gathered not just about the individual user, but about people around them as well. Thus, a solely consent-based model does not entirely ensure the protection of one's data, especially when data collected for one purpose can be repurposed for another."

While mapping of the data submitted by the individual may generate big data bases, the circumference of which is often unknown to the individual, right to privacy acts as shield from unreasonable intervention with her data. Her profile may be carved out and exposed where little secrecy is possible. The moment she uses internet for visiting sites, items of advertisement pop up creating an instinct to visit the sites or disrupt her from carry on with her activity for which she used the internet. Can she therefore be deprived of accessing internet directly or indirectly?

The state requires the data from public for better 'social and economic ordering'.[17] The state needs to monitor the data for national security reasons. Is there a compelling state necessity to access data from individuals? If yes, how do we balance the two kinds of interests, namely, the interest of the individual for maintaining privacy and protection of state interest. Presumably, the state interest is for the welfare of the individual. The critiques of Aadhaar are worried about the ability of the state to maintain secrecy/protection of the data of the individual. Can the inability of the state be cited as a reason to deny the state access to the data of the individual? Can the inability of the state be a reason for denial of right to privacy to the individual? During the course of arguments, the Learned Attorney General of India argued in favour of retention of the findings of the Court in M.P. Sharma and Kharak Singh. He referred to the Constituent Assembly Debates in detail to show that the founding fathers of the Constitution did not include right to privacy in the fundamental rights part of the Constitution.[18] This led to a debate whether the Founding fathers deliberately avoided its inclusion or Part III remained silent on the matter. As per Justice Chelameswar, a close scrutiny of the debates reveals that the Assembly only considered whether there should be an express provision guaranteeing the right of privacy in the limited context of 'searches' and

---

[16] *See* Yvonne McDermott, *Conceptualising the Right to Data Protection in an Era of Big Data*, 4 (1) BIG DATA AND SOCIETY 1-7 (2017). Quoted by Chandrachud J. at para 173.

[17] Christina P. Moniodis, *Moving from Nixon to NASA: Privacy's Second Strand- a Right to Informational Privacy* 15 (1) YALE JOUR. L. & TECH. (2012).

[18] *Supra* ('privacy judgment') note 1, at para 6, (Opinion of Nariman J.).

'secrecy of correspondence'.[19] Dimensions of the right of privacy are much larger and were not fully examined.[20]

The question whether the expression 'liberty' in Article 21 takes within its sweep the various aspects of the right of privacy was also not debated.[21] The Attorney General argued against placing right to privacy, a part of personal liberty above the right to life. He also argued that people shared so much information in the public domain, there is hardly anything left for protection by the State.[22]

As explained above, e-governance is a well-appreciated mode of governance which reduces visible governmental control. Individuals/citizens shall muster the courage to perform their duties to the state as part of their social contract with the state. Democracy does not end in enrolment as a voter, participating in election or choosing a government. Individual's participation in a democracy is yet to be fully realized in India. While free and fair elections form part of an essential component of democracy, the prosperity and vibrancy of democracy depends on vigilant citizens of the democracy. An effective way of creating such a democracy is by entrusting citizens with fulfilling their duties in a democracy. Their direct participation through e-governance measures build up their confidence and they realise the importance of themselves being part of nation building. The state may need data from them for conferring social benefits and ensuring that the benefit reaches the right person; the state may require information about tax evaders; the state may require prevention and investigation of crime and for many other state interests[23]. Therefore, the compelling state necessity to access the data of the public is clearly established.

The Court refers to the distinction between anonymity and privacy maintained by the contemporary literature[24]. If the state uses the medical records of an individual for public health reasons while maintaining the anonymity of the individual, it may be considered as a legitimate state interest. The state may use this data for adopting appropriate strategy to address public health concerns like the outbreak of dengue, and swine flu.

---

[19] *Supra* ('privacy judgment') note 1, at para 17, (Opinion of Chelameswar J.); *See also* Granville Austin, THE INDIAN CONSTITUTION: CORNERSTONE OF A NATION 72(1966).

[20] *Id.*

[21] *Id.*

[22] Para.6.

[23] *Supra* ('privacy judgment') note 1, at para 181, (Opinion of Dhananjay Chandrachud J).

[24] *Id*. at para 182.

Requirement for Data Protection

The Court highlighted the study conducted by the erstwhile Planning Commission of India on data protection.[25] The Expert Group constituted by the Planning Commission considered the salient features of the proposed data protection law as follows:[26]

(a) Technological neutrality and interoperability with international standards;
(b) Multi-dimensional privacy;
(c) Horizontal applicability to state and non-state entities;
(d) Conformity with privacy principles; and
(e) Co-regulatory enforcement mechanism.

The Expert Group developed principles of privacy as follows:[27]

(i) *Notice*: A data controller shall give simple-to-understand notice of its information practices to all individuals in clear and concise language, before personal information is collected;
(ii) *Choice and Consent*: A data controller shall give individuals choices (opt-in/opt-out) with regard to providing their personal information, and take individual consent only after providing notice of its information practices;
(iii) *Collection Limitation*: A data controller shall only collect personal information from data subjects as is necessary for the purposes identified for such collection, regarding which notice has been provided and consent of the individual taken. Such collection shall be through lawful and fair means;
(iv) *Purpose Limitation*: Personal data collected and processed by data controllers should be adequate and relevant to the purposes for which it is processed. A data controller shall collect, process, disclose, make available, or otherwise use personal information only for the purposes as stated in the notice after taking consent of individuals. If there is a change of purpose, this must be notified to the individual. After personal information has been used in accordance with the identified purpose it should be destroyed as per the identified procedures. Data retention mandates by the government should be in compliance with the National Privacy Principles;
(v) *Access and Correction*: Individuals shall have access to personal information about them held by a data controller; shall be able to seek correction, amendments, or deletion of such information where it is inaccurate; be able to confirm that a data controller holds or is processing information about them; be able to obtain from the data controller a copy of the personal data. Access and correction to personal information may not be given by the data controller if it is not, despite best efforts, possible to do so without affecting the privacy rights of another person, unless that person has explicitly consented to disclosure;
(vi) *Disclosure of Information*: A data controller shall not disclose personal information to third parties, except after providing notice and seeking informed consent from the individual for such disclosure. Third parties are bound to adhere to relevant and

---

[25] *Id*. at para 184.
[26] *Id*.
[27] *Id*.

applicable privacy principles. Disclosure for law enforcement purposes must be in accordance with the laws in force. Data controllers shall not publish or in any other way make public personal information, including personal sensitive information;

(vii) *Security*: A data controller shall secure personal information that they have either collected or have in their custody, by reasonable security safeguards against loss, unauthorised access, destruction, use, processing, storage, modification, de-anonymization, unauthorized disclosure [either accidental or incidental] or other reasonably foreseeable risks;

(viii) *Openness*: A data controller shall take all necessary steps to implement practices, procedures, policies and systems in a manner proportional to the scale, scope, and sensitivity to the data they collect, in order to ensure compliance with the privacy principles, information regarding which shall be made in an intelligible form, using clear and plain language, available to all individuals; and

(ix) *Accountability*: The data controller shall be accountable for complying with measures which give effect to the privacy principles. Such measures should include mechanisms to implement privacy policies; including tools, training, and education; external and internal audits, and requiring organizations or overseeing bodies extend all necessary support to the Privacy Commissioner and comply with the specific and general orders of the Privacy Commissioner.

The above mentioned privacy principles fixes the parameters within which the data usage shall be permitted. These principles accommodate the concerns expressed by the proponents and opponents of Aadhaar linkage. Any deviation from any of the principles stated above may disrupt the credibility of the linkage and perception of state as the protector of public interest. These principles are as carefully designed similar to the guidelines adopted by the Indian Council for Medical Research and the protocols followed in medical institutions for administering treatment. The attitude of clinical precision maintained by the Expert Group while developing and recommending these principles reflect on the sensitivity of the individual claims and the heavy accountability to be undertaken by the state on usage of the data of its subjects.

Privacy under Article 21 and the Due Process Compliance

The Court maintained that right to privacy is covered under Article 21 of the Constitution. This mandates the application of due procedure stipulated in Maneka Gandhi [28] and thereafter. Any violation of right to privacy can be justified by a constitutionally legitimate law which lays down a procedure just, fair and reasonable. The law must fulfil reasonableness test under Article 14 of the Constitution to resist arbitrary state action. In other words, compelling state interest does not permit arbitrariness on the part of the state. The means deployed by the state shall be proportional to the object and needs stipulated in the law.

The Court's decision to place the right to informational privacy under Article 21 may be considered as an effort to safeguard the right in the best constitutional sense. The judicial

[28] *Maneka Gandhi* v. *Union of India* (1978) 1 S.C.C. 248.

review operates on any executive or legislative action on access to data base. The constitutional courts of India will determine the reasonableness of such actions and the requirements of due process under Article 21 of the Constitution. The necessity and proportionality of such actions should be justified by the state.

Conclusions

The discourse on the right to informational privacy by the Court took place at an appropriate time. India has entered the path of e-governance. The sectors like education, health and utility services are adopting information technology based operation. The data on internet subscription shows the interest of the people to move towards information technology based operations. It may be true that people may have given up their data by exercising their choice in favour of internet based services as argued by the Attorney General of India in this case. Even if that be so, can the state deny the right to privacy of people with respect to their data?

The Court deliberated on the contours of right to privacy in the case to examine the feasibility of a privacy claim in the information age and compelling state interest. Justice Chelameswar in his separate opinion stated that the theory of compelling state interest originated in the United States. The strict scrutiny test followed by the United States consisted of two elements, namely, compelling state interest and narrow tailoring.[29] He observed that compelling state interest does not have specific contours in the United States and therefore, it is imperative to adopt this standard with clarity as to when and in which type of privacy claims it is to be used.[30]

Justice Nariman on elaborating the contours of the right to privacy referred to an article published in the California Law Review of 1976.[31] This article explains the intricacies of the debate. The three components of the right to privacy explained by the author in the article are repose, sanctuary and intimate decision. As per the article, repose maintains the individual's peace; sanctuary allows an individual to keep some things as private; and intimate decision grants the freedom to act in an autonomous fashion. In the words of the author,

> '…Whenever a generalized claim to privacy is put forward without distinguishing carefully between the transactional types, parties and courts alike may become hopelessly muddled in obscure claims. The clear standards that appear within each zone are frequently ignored by claimants anxious to retain some aspect of their personal liberty and by courts impatient with the indiscriminate invocation of privacy.
>
> Finally, it should be recognized that the right of privacy is a continually evolving right. This Comment has attempted to show what findings of fact will

---

[29] See *M. Nagaraj* v. *Union of India* (2006) 8 S.C.C. 212; *Ashoka Kumar Thakur* v. *Union of India* (2008) 6 S.C.C. 1 (These and similar cases contains detailed discussion on the 'tests').

[30] *Supra* ('privacy judgment') note 1, at para 45, (Opinion of Chelameswar J.).

[31] Gary Bostwick, *A Taxonomy of Privacy: Repose, Sanctuary, and Intimate Decision* 64 CALIF. L. REV. 1447(1976).

> lead to the legal conclusion that a person has a right to privacy. Yet the same findings of fact may lead to different conclusions of law as time passes and society's ideas change about how much privacy is reasonable and what kinds of decisions are best left to individual choice. Future litigants must look to such changes in community concerns and national acceptance of ideas as harbingers of corresponding changes in the contours of the zones of privacy'.

Justice Nariman referred to the vagueness associated with privacy by classifying the right to privacy in three categories, namely, privacy of the person's body, privacy of the person's mind (informational privacy), and the privacy of choice (individual's autonomy over personal choices).[32] The first category may be protected by Article 19(1)(d); and (e) with Article 21 of the Constitution. The second category may be offered protection under Article 21. The third category falls under Articles 19(1)(a) to (c); 20(3); 21; and 25 of the Constitution.[33]

The nuances of privacy claim as a right was explained by Justice Mathew in Gobind case.[34] This Court took cognizance of those nuances. Justice Mathew while delivering the judgment of the Court stated that our Constitution makers wanted to ensure conditions favourable to the pursuit of the happiness of the individual.[35] However, Justice Mathew was cautious to rely on a broad definition of privacy that is not explicitly stated in the Constitution. Therefore, he stated that an important countervailing interest should be shown in the form of compelling state interest to deny the privacy claim of the individual.[36]

In view of the above discussion, the Court in Puttaswamy case decided to adopt a middle path. The Court found some aspects of privacy debate to be serious enough for judicial intervention. The Court also found the claims of the state for access to data base as genuine in the contemporary era. The Court wanted to strike a right balance between the individual and state interests. The extent of success of such balance will depend upon the constitutionality of the data protection law to be enacted by the state.

- Meena S. Panicker[**]

---

[32] *Id*. at para 81.

[33] *Id*.

[34] *Gobind* v. *State of Madhya Pradesh* (1975) 2 S.C.C. 148.

[35] *Supra* ('privacy judgment') note 1, at para 48, (Opinion of Chandrachud J.

[36] *Id*. at para 49

[**] Assistant Professor of Law, University of Delhi. Email: meenapanicker@gmail.com