PRIVACY AND CITIZENSHIP IN INDIA: EXPLORING CONSTITUTIONAL MORALITY AND DATA PRIVACY

Dr. Nupur Chowdhury[*]

This paper maps the current landscape of the nature and scale of the use of digital media in India through relationship typologies between citizens, intermediaries and the State. These typologies help explain the gamut of functions, both private and public in nature, which the internet has enabled in India. The implications of these typologies are sought to be understood in the broader context of judicial developments vis-à-vis the right to privacy. This study is undertaken with the acknowledgement that the State's emerging role in large scale data collection and identity verification through projects like 'Aadhaar' indicates that as we navigate the terrains of data privacy, the Indian State itself is not a disinterested regulator on the issue of privacy. The Supreme Court's recent recognition of the right to privacy as a fundamental right under the Indian constitution provides for an expanded terrain to develop taxonomy of privacy violations. This necessitates the adoption of a rigorous standard of review by referencing ideas of human dignity and democracy embedded within the conception of constitutional morality.

I. INTRODUCTION

In June 2017, a newspaper reported how an experiment relating to privacy had given the Alipore Zoo in Kolkata its first crocodile hatchlings in a decade. The report cited privacy being accorded to the resident mating pair as the reason behind seven hatchlings becoming new occupants of the isolated enclosure of the marsh crocodiles.[1]

---

[*] Assistant Professor, Centre for the Study of Law and Governance, Jawaharlal Nehru University, New Delhi, India. Email: nupur@jnu.ac.in

I am indebted to Dipika Jain, Ray Sharat Prasad, P. Puneeth, Ghazala Jamil, Nidhi Srivastava, Ioanna Tourkochoriti, Adrian Athique, Vibodh Parthasarathi, Aasim Khan and the Editorial Board, NUJS Law Review for discussions and comments on this paper. Earlier versions of this paper were presented in the International Symposium on the India Media Economy, IIT-Bombay, December 6-8, 2017 and at the International Symposium on Digital Politics in Millennial India, IIIT-Delhi, March 15-17, 2018 and I benefitted immensely from the comments by participants at both these symposiums. I acknowledge discussions with Nishtha Sinha and Rohit Sarma specifically on the idea of Constitutional Morality. This research was supported by the Indian Council of Social Science Research (ICSSR Grant No. 02/280/2016- 17 /Rp – Responsive Research Project – "Law, Technology and Development: Theoretical Explorations and Case Studies").

The responsibility for the facts stated, opinions expressed, and conclusions drawn are entirely mine.

[1] Debraj Mitra, *Croc-a-hoop at the zoo*, The Telegraph (Kolkata) June 26, 2017.

It appears that not only humans but also those in the animal kingdom value their privacy and can, therefore, expect to secure privacy through human intervention if their privacy can result in certain ostensibly 'productive activities'. The intriguing question is whether the individual right to privacy should hinge on the productiveness of the activities that are undertaken in private? State intervention and interruption of this privacy has long been justified in the case of social harms that may result from the practice of privacy. Yet that is a negative condition.[2]

Privacy as a positive obligation, for the performative, denudes the very idea of individual autonomy, which the right to privacy seeks to secure and nurture.[3] Privacy is also envisaged as a positive condition if the State is in a position to determine and differentiate between good and bad privacy.[4] Good privacy would relate to cases in which the State can suitably establish that there is absence of public harm and bad privacy would be determined when it results in public harm. However, arguably the trouble with anointing the State with authority to make this determination is that it may result in first, the rapid expansion of the category of activities which result in public harm (including gauging the potential impact of activities) and second, it would also provide the State with a justification for authoritatively determining for what purpose good privacy should be used.[5] This indeed would in effect turn the citizenry into subjects.

It is critical therefore, to review the claim that privacy is just a performative. It is in essence a quality of autonomy to act or desist from acting in pursuit of one's individual ends.[6] Embracing notions of the perfomative only provides the State as a *fait accompli* to expand its jurisdiction and powers in determination and enforcement of limits to privacy in the name of public interest without necessary cause or even procedural due diligence. It also raises the question whether there are any limits to the State's *suo motu* determination and takings of such privacy interests and rights from the individuals. More provocatively, one needs to reflect on whether philosophically speaking there can be any limits to privacy intrusions and takings by the State and non-State actors. Are there any core areas of individual autonomy and decision-making which are sacrosanct and of which such intrusions or takings cannot be tolerated or ever justified?

---

2 Laurence D. Houlgate, *What Is Legal Intervention in the Family? Family Law and Family Privacy*, 17(2) Law and Philosophy 141-158 (1998).

3 Debra Morris, *Privacy, Privation, Perversity: Toward New Representations of the Personal*, 25(2) Signs 323-351 (2000).

4 *See*, *e.g.*, the social credit scheme in China, Meg Jing Zeng, *China's Social Credit System puts its people under pressure to be model citizens*, Conversation (Australia edition), January 24, 2018, available at http://theconversation.com/chinas-social-credit-system-puts-its-people-under-pressure-to-be-model-citizens-89963 (Last visited on February 20, 2019).

5 Elin Palm, *Privacy Expectations at Work—What Is Reasonable and Why?* 12(2) Ethical Theory and Moral Practice 201-215 (2009).

6 J. Angelo Corlett, *The Nature and Value of the Moral Right to Privacy* 16(4) Public Affairs Quarterly 329-350 (2002).

India has one of the fastest growing markets in terms of internet access and connectivity in the world.[7] This expansion has been primarily led by the growth in mobile telephony. The mobile telephony market has been fiercely competitive with new players like Jio Telecom entering the market thereby further driving down prices in an already highly price sensitive market.[8] Nevertheless, internet penetration still continues to be limited to not more than 35% of the Indian population.[9] This is an important figure to keep in mind while discussing the issue of privacy on the internet in the context of India. Often discussions of privacy in India and the lack of protection thereof is assailed by charges of elitism and privilege[10] but as our discussion will show this is a fig leaf because privacy is not just a public policy issue for those Indians who have access to the internet but should be of concern for everybody else as well. This is because the use of the internet to access public and private services has expanded rapidly through the Digital India project and the perverse incentives created by the official use of private services to address all forms of public outreach including grievance redressal.

One way to address this issue is to provide a descriptive analysis of internet usage in terms of typologies of relationships between citizens, other non-state actors and the State. In examining these relationships, it is critical to address two conceptual hurdles. First, what is the implication of privacy in the internet era? Second, if privacy is really a personal asset of the individual, why broaden the canvas to examine the implication of these personal choices on structural relationships between states and citizens or even between citizens and markets? Both these aspects are discussed in the following sections.

A. TWO CONCEPTUAL HURDLES

Coming to the first issue, the use of the term 'internet era' is deliberate in drawing attention to the qualitatively different aspects of the relationships/transactions that are embedded within the domain of the internet. The increasing reach of the internet both in terms of its physical access to users[11] and in terms of

[7] Rishi Iyengar, *The future of the internet is Indian*, CNN Business, November 2018, available at http://edition.cnn.com/interactive/2018/11/business/internet-usage-india-future/ (Last visited on February 2, 2019).

[8] Ivan Mehta, *Reliance Jio Is Driving Indian Internet Growth, Says The Mary Meeker Report*, Huffpost (India), June 2017, available at https://www.huffingtonpost.in/2017/06/01/reliance-jio-is-driving-indian-internet-growth-says-the-mary-me_a_22120777/ (Last visited on February 20, 2019).

[9] IAMAI & Kantar IMRB, *Mobile Internet Report in India* (2017). (Overall internet penetration was 35% of the total population as on December 2016).

[10] *See*, *e.g.*, Krishnadas Rajagopal, *Major Arguments In The Right To Privacy Case*, The Hindu, August 24, 2017, available at https://www.thehindu.com/news/national/major-arguments-in-the-right-to-privacy-case/article19551038.ece (Last visited on February 20, 2019). (Highlighting the arguments of the Attorney-General K.K. Venugopal for the Central government)

[11] The Digital India initiative is designed to ensure internet access to every Indian by not only ensuring physical access but also incentivizing access by linking public information and social entitlements on the internet. This is being pushed aggressively by the Government of India by not only prescribing Aadhaar (identification numbers based on biometric and demographic data) but

the nature of social and economic transactions that it engenders is qualitatively different from that in the physical world.

Let us take an analogy. Although overtly the internet resembles a physical market place, where individuals transact (buy and sell goods and services), it also is marketed as a "public space"[12], a source of news (function that is traditionally performed by newspapers and broadcasting media) and is also a place of leisure. These multiple functionalities are what makes the internet truly different from any other concomitant physical space and also explains its attractiveness and usefulness.[13] Yet, this is also a space which is under acute surveillance in terms of accumulation of footprints of individual users and allows for the creation of fairly accurate profiles of individual users based on their activities online. This is premised on the social contract that free services are provided for access to personal information which is legitimised through the consent that is provided by individual users.

It is critical to understand the material nature of the consent sought and the consent given by users to understand the implications of "consent as is practiced" in the digital space of the internet. Consent is usually sought in an episodic manner for specific transactions and is presumed in perpetuity. The nature of the market itself, in terms of platform players like Facebook or Google, which allows for multiple functionalities means that it is fairly easy to create deep user profiles based on individual consent specific transactions. The nature of these user profiles is fairly deep in terms of not only pedestrian habits, but also political views, sexual orientations, biological information and medical history amongst other personal information.[14] Are these user profiles essentially 'benign'; i.e. they are merely used to provide information to advertisers so as to better target the marketing of goods and services or equip them to provide for improved user experience? As is evident

---

also allowing for private intermediaries to use the platform for authentication for provisioning of private goods and services.

Consider, IndiaStack initiative of not-for-profit think tank iSPIRT "allows governments, businesses, startups and developers to utilize an unique digital Infrastructure to solve India's hard problems towards presence-less, paperless, and cashless service delivery. The Open API team has been a pro-bono partner in the development, evolution, and evangelisation of these APIs and systems." *About*, India Stack, available at https://indiastack.org/about/ (Last visited on February 20, 2019).

The lynchpin of the digital infrastructure is the use of Aadhaar number to verify identity for a host of transactions to access goods and services. Thus although the Aadhaar was ostensibly designed to address "dissipation of social benefits" its uses have been expanded rapidly to not only other public services (see filing income tax) but also accessing private goods and services.

[12] Consider the advertisements of Facebook inviting people to come find companions, meet new people and form associations with others on their webpage.

[13] It also raises the question as to whether the same public expectations and social values that regulates the role of traditional news media (paper and broadcasting) apply to new media in terms of its role as news reporters.

[14] The idea of Big Data is essentially this convergence of the possibility of foot printing users to create a user profile that provides an indelible insight into the identity (biological, thought and action) of individuals using their activities on the internet to make approximate predictions about their personality.

in any fairly straightforward legal analysis of standard consent forms found in signing up for "free services" such as Gmail, Research Gate, Word Press, Facebook or Instagram, even such benign motives are never revealed in a sufficiently clear and understandable manner. In reality, therefore, "consent as is practiced" is neither informed (which would entail allowing users to make a decision with all necessary information about the grounds, implications and outcomes of the consent) nor substantive.

What does "substantive" mean? Real consent would allow an opportunity for the individual to not be substantially affected or harmed by not giving consent. It can be explained as counter factual. Only if consent can be withheld without incurring any grave personal harm does the giving of consent become free and therefore, valid and effective in terms of an expression of personal autonomy.[15] Otherwise consent is given under duress and therefore, usually considered legally invalid.

Given that internet penetration is rapidly increasing and a substantial portion of our social life is now on the internet (including employment opportunities) and arguably it is increasingly difficult (if not impossible) to not use the internet (and in the process consent to "free services") in the face of potentially grave personal harm or loss of employment opportunities in terms of foregoing both public services and private goods and services. Consent then is nugatory and only functions to render a patina of legitimacy to violations of privacy.

The social contract of free services for personal information is, therefore, quite simply an invalid contract. Further, there is a significant potential for grave personal harm in terms of silent ascription of identities through user profiles which can then become a ground for denial of civil liberties (predictive policing, online censorship of speech and expression) if these become the basis for profiling and policing or for even creating disadvantage and discrimination in social relations through silent ascription of identities which users will not have an opportunity to challenge, contest or resist.[16] In effect, this represents the end of the right to due process.

---

[15] The same can be argued in the context of the Aadhaar project which is legitimated on the basis of consensual parting of biometric information to access social entitlements. However, in practice consent as is practised is rendered illusory through executive actions making it mandatory even in other cases wherein there is no question of accessing such benefits.

[16] The silent nature of these ascriptions is conditioned by the information asymmetries structural to the internet and consequently also denudes the individual from any opportunity of challenging them. See Frank Pasquale, Black Box Society (2015). (For an extensive discussion of the impact of decision making by algorithms on the social life of individuals). I eschew the term data as it semantically obfuscates the fact that it is essentially personal information that reveals the identity of the person. Ascription of identity through profiling without any possibility to challenge was also practiced by the colonial state – for instance under the Criminal Tribes Act, 1871. (I am indebted to Dr. Aasim Khan of IIIT Delhi for suggesting to me this point which curiously highlights the continuity between a colonial state and the present Indian state)

This brings to us to the next conceptual hurdle. If social life, as is practiced currently will increasingly be practiced in digital India, requires citizens to become users of the internet, then it is imperative that we evaluate the implications of the social contract and in turn 'consent as is practiced' not only in terms of possible harms to individuals but also in terms of cumulative harms to the Constitutional republic itself (through the idea of constitutional harms). The latter can be understood in terms of structurally challenging the relationship between the State and citizen as is imagined and regulated by the pre-eminent social contract i.e. the Constitution of India (in terms of the values of human dignity, democracy and civil liberties like freedom of speech and expression, embedded in it).

In this context, the reaffirmation of the fundamental right to privacy under the Constitution of India, explicitly stated by the nine judges of the constitutional bench of the Supreme Court[17] provides us with an opportune moment to undertake a number of explorations. What are the constitutional implications of this recognition? This was first applied to review a claim that the Aadhaar project (the State providing unique identity numbers to all residents in India based on their biometric details (iris scan and finger prints)) was in violation of the right to privacy. The Court upheld the Aadhaar project with certain conditions[18] on the ground that dissipation of social benefit due to failure to establish identity was a serious problem. Therefore, it was of legitimate State interest to develop and implement Aadhaar and so it fulfilled the test of proportionality as there was no other less restrictive but equally effective alternative measure available.[19] Although the Aadhaar project is developed by the State, its use by the private actors for identity verification has expanded rapidly. To the extent that the government has recently brought in an Amendment Bill in the Parliament to the Aadhaar Act, 2016 to circumvent the Court's reading down of specific provisions allowing for use of Aadhaar by private actors.[20]

---

[17] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

[18] One of the conditions was the enactment of a Data Protection Act which would ensure minimum protections in terms of laying down conditions for collection and deployment of personal data. Following this signal from the Court, the government had established the Justice Srikrishna Committee to draft a Bill, which was made public available for comments in July 2018. The Bill has since then been pending with the government and is expected to be introduced in the forthcoming Budget Session of the Indian Parliament (Winter 2019). The Executive has delayed introducing the Bill in the Parliament and has attracted justifiable criticism that it is not interested in even providing minimum protections to the public, given that it is also invested and pursuing projects that allow for indiscriminate collection (without probable cause) and surveillance of personal data.

See, e.g., Ministry of Home Affairs, Order S.O. 6227(E) (December 20, 2018) issued in exercise of powers under Section 69(1) of the Information Technology Act, 2000 and Rule 4 of the Information Technology (Procedure and Safeguards for the Interception, Monitoring and Decryption of Information) Rules, 2009 authorising an expanded number of security and intelligence agencies to intercept, monitor and decrypt any information generated, received, transmitted or stored in any computer resource in India.

[19] K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1 : 2018 SCC OnLine SC 1642 (Aadhaar judgment).

[20] *See* Aadhaar and Other Laws (Amendment) Bill, 2018 passed in the Lok Sabha (lower house of the Parliament), pending in the Rajya Sabha.

The Aadhaar judgement of the Court reflects its failure to appreciate the current reality of how information is collected, stored and shared and also the (in)ability of individuals to assess and negotiate singular actions of information sharing and differentiating them from the cascading effects of information merging and the potential harms which may result from the abuse of such data convergence. This failure is also more problematically reflected in the continued emphasis on individual consent as the fundamental principle for allowing for privacy intrusions, when in fact individuals have little knowledge, information or agency in negotiating such acts of sharing of privacy.

In this context this paper undertakes the following explorations.

First, there is an attempt to understand the nature of the digital space as is experienced and actively participated by Indian citizens. I develop a typology of relationships in the digital space between the State, citizens and non-state actors (private intermediaries). Given that the digital space is primarily constructed on the social contract that free services are provided for access to personal information, the issue of privacy is better understood through the appreciation of relationships in the digital space. The typology provides a descriptive window into 'consent as is practiced' in the digital space in India.[21] It not only establishes a conceptual structure in relation to relationships on the internet in order to frame the regulatory debates relating to privacy therein, but also underlines the critical linkages between these framings. These critical linkages are reflected not only in law and policy but also help in explaining and appreciating executive (in)actions and judicial interventions in this context.[22]

Second, in order to effectuate a fundamental right to privacy, it is critical to distinguish between species of privacy violations as not all violations impose equal restrictions on the individual. In this context I suggest that we need to differentiate between privacy takings and privacy intrusions.

Third, I explore the standard of judicial review which such privacy violations should attract. I argue that the discourse on fundamental rights will be substantially enriched if we reference the idea of constitutional morality as an intellectual resource to provide constitutional compass to our discussions on the standard of review.

This article is divided into five parts. Part II maps the relationship typologies played out between three primary groups – the State, citizens and

[21] *See* Thomas P. Crocker, *Ubiquitous Privacy*, 66 Okla. L. Rev. 791 (2014). (Arguing that it is important to understand the value of privacy in a specific social context)

[22] The Government of India's push for the Aadhaar project is also responsible for its on timidity in pursuing privacy violations *inter se*. Similarly the adoption of private social media platforms by public functionaries may also undermine their willingness to regulating their behaviour. This makes the Executive an interested party and not just a disinterested or neutral regulator on discussions on privacy.

intermediaries. Part III explores the jurisprudence on privacy in India. It is critical to appreciate the fact that courts will play a formative role in regulating of the internet more generally and specifically on the issue of privacy in the digital world. Indeed this is being widely recognised by academicians across disciplines.[23] Part IV reflects on the Indian legislative conceptualizations of privacy and its impact in shaping relationships in the digital world. It brings these two previous discussions on privacy together in the context of the constitutional objectives of dignity and democracy. Finally, in the Part V some concluding remarks are forwarded on privacy in the context of constitutional morality.

However, before embarking on such an exploration, it is important to make a caveat. I am well aware that there are cognitive uncertainties in delving into jurisdictional ideas of privacy in the digital world. Nevertheless, I will defend this as a necessary endeavour, given that digital relationships will impact our offline relationships and in the process recast and fundamentally redefine the relationship between the citizen and the State.

II. INTERNET RELATION TYPOLOGIES

There is a material difference between how privacy is both imagined and practiced in the digital world as compared to our physical world.[24]

While defending expanded powers of the State to police private behavior on the internet, Additional Solicitor General, Mr. Tushar Mehta relied on this argument to show the increasing propensity of the internet as a medium of communication to violate privacy of individual users.

> "In case of media like print media, television and films, it is broadly not possible to invade the privacy of unwilling persons. While in the case of an internet, it is very easy to invade upon the privacy of an individual and thereby violating his right under Article 21 of the Constitution of India."[25]

This is the core of the argument for treating internet as a different medium. It is a medium that is designed to enhance certain human proclivities and allows for extremely intrusive and far reaching data gathering of user information.[26] These proclivities are further exacerbated with the rapid expansion of

---

[23] A. Callamard, *Are courts re-inventing Internet regulation?* 31 International Review of Law, Computers & Technology 323 (2017).

[24] *See* Frederick Schauer, *Internet Privacy and the Public-Private Distinction*, 38(4) Jurimetrics 555-64 (1998). (For an excellent discussion on the differences between internet privacy and privacy of physical spaces)

[25] Shreya Singhal v. Union of India, (2015) 5 SCC 1, ¶30.

[26] *See e.g.,* Frank Webster, *The Intensification of Surveillance* in The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age (Ball Kirstie & Webster Frank ed.) 1-15 (2003); Carly Nyst, *Secrets and Lies: The Proliferation of State Surveillance Capabilities and*

internet usage in India not only by private citizens pursuing their own ends but also it increasingly becoming a tool of governance itself and therefore in ordering relationships between citizens and the State.

These typologies are put into three categories. First, is the increasing usage by government agencies and ministers of private platforms to communicate and also undertake public services delivery and grievance redressal. Instances of this include the Minister of External Affairs rescuing of immigrant Indians in foreign countries through her Twitter account and ministers taking cognizance of Change.org petitions to push for policy changes. It has also resulted in conflict resulting from Governors of States bypassing the Chief Minister's office to issue executive commands directly to the bureaucrats.

Second, is that there has been a trend of excessive reliance on intermediaries (both internet service providers (ISPs) and content providers like Google, Facebook and Twitter) by the government agencies in seeking to regulate unlawful content over the internet.[27]

The third set of relationships is between users, in this case citizens, and the intermediaries, wherein there is a contractual relationship of usage of certain services that allow citizens to access and use the internet for a number of functions. Arguably this category is amongst the most private in nature in terms of the legal relationship between the parties. Yet, as we shall see, it is critical that all these relationships are seen in concomitance with each other. Therefore, necessarily their implications on citizen's rights and responsibilities are manifold. This will become clear in the following discussion on each of these three relationships.

A. STATE AND CITIZENS

The first aspect requiring our consideration is the rapid embrace of social media by public entities. The executive in India has been prolific in using private platforms like Twitter and Facebook to interact directly with users. For instance, the Minister for External Affairs Sushma Swaraj was named Global

the Legislative Secrecy Which Fortifies Them – An Activist's Account State, 7(1) Crime Journal 8-23 (2018); Neil M Richards, *The Dangers of Surveillance*, 126(7) Harvard Law Review 1934-1965(May 2013). *See* Matthew Hindman, The Internet Trap: How the Digital Economy Builds Monopolies and Undermines Democracy (2018).

[27] *See e.g.*, Amrita Vasudevan, *Taking Down Cyber Violence: Supreme Court's Emerging Stance on Online Censorship and Intermediary Liability*, 54(2) Economic and Political Weekly (2019); Divij Joshi, *Beyond Intermediary Liability: Platform Responsibility for Harmful Speech in India*, Digital Policy Portal, November 3, 2018, available at http://www.digitalpolicy.org/beyond-intermediary-liability-platform-responsibility-for-harmful-speech-in-india/ (Last visited on February 2, 2019). (Both discussing the risk of overreach by intermediaries while taking down harmful content, specifically when delegation of such competence by the State is without adequate supervision)

Thinker in 2016 for "novel twitter diplomacy" by Foreign Policy Magazine.[28] Similarly the Prime Minister (Shri Narendra Modi) and his cabinet ministers like Arun Jaitley (Minister of Finance) and Suresh Prabhu (Minister of Railways) and Piyush Goyal (Minister of Power) are especially prolific on social media.[29] Apart from this, various government agencies ranging from Delhi Traffic Police to that of regulatory bodies like TRAI (Telecom Regulatory Authority of India) as well as the Election Commission of India are active users of social media. Further, the Government of India has unveiled the Digital India project to push expansion of public services delivery and private financial transactions over the internet. On the face of it this has been lauded by the media and other public commentators but there has also been notable backlash.

In January 2017, the Government of Puducherry, a Union Territory issued an administrative order mandating as follows:

> "Hon'ble Chief Minister, Puducherry has noted that many Officers are using digital mode and social media such as Facebook, WhatsApp, Twitter, etc., for official communication. The servers of these multinational companies are based outside the country. Therefore, any foreign country can get these official communication and documents uploaded therein. This is violation of Official Secrets Act and also against the guidelines issued by the Ministry of Information Technology, Government of India, New Delhi.
>
> Hon'ble Chief Minister has directed that all Government Officers/officials and employees of Societies/Organisation run by Government shall desist from use of such social media for official works. No group sha11 be formed for official communication and they should not be members of any official group run in such social media nor interact with seniors bypassing the Administrative hierarchy and routine official channel. Strict compliance should be ensured by all concerned and violation, if any, of these instructions brought to notice shall invite

[28] Shailaja Neelakantan, *For 'novel Twitter diplomacy', Sushma Swaraj named a 2016 'Global Thinker' by Foreign Policy magazine*, The Times of India, December 14, 2016, available at http://timesofindia.indiatimes.com/india/for-novel-twitter-diplomacy-sushma-swaraj-named-a-2016-global-thinker-by-foreign-policy-magazine/articleshow/55974675.cms (Last visited on February 20, 2018).

[29] *See*, *e.g.*, Dhanya Ann Thoppil, *Meet Modi's Social Media Men*, Wall Street Journal Blog, July 5, 2013, available at https://blogs.wsj.com/indiarealtime/2013/07/05/meet-modis-social-media-men/ (Last visited on February 2, 2019); Press Information Bureau Press Release, *I&B Minister Writes to Ministries to Come On Social Media Platforms through the Already Established Communication Hub*, 30 May 2014, available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=105307 (Last visited on February 20, 2019).

> disciplinary action and further penal action as per rules in force."[30]

This order was thereafter cancelled by the Lieutenant Governor of Puducherry, Kiran Bedi, as it was in contravention of relevant guidelines, rules and policies. Furthermore, she added on Twitter that "If Puducherry has to be a progressive UT, it cannot be retrograde in communications. Hence @CM_ Puducherry's order stands cancelled:@PMOIndia (sic)"[31]

It is to be noted that Puducherry has the constitutional status of a Union Territory, and like Delhi, is governed by Lieutenant Governor, who is essentially the representative of the Union Government. It also has an elected state assembly with the Chief Minister heading the executive.[32] It is argued that this exchange apart from illustrating the constitutional problems of sharing governing powers between an elected representative and an unelected governor, also gives us a window into the evolving ethics of using private media for public communication and governance.

Let us deconstruct this a bit further. Transparency in governance is likely to receive support from most citizens. Therefore, efforts at increasing transparency and communication of such government actions are widely applauded. However, let us pause for a moment to consider the following hypothetical situations.

1. Situation 1—Tweet for Assistance

Nakul, Arjun and Sahadev are all Indian immigrants working in Qatar. Nakul is working in the construction sector, Arjun is working as a management consultant and Sahadev is a yoga practitioner. Nakul is literate but not educated enough to navigate the internet since it presumes a working knowledge of English, while both Arjun and Sahadev are active users of the internet. All the three immigrants lose their employment and, subsequently, their labour contractors confiscate their passports. Arjun is a Twitter user and is able to immediately contact the Indian Minister of External Affairs on its Twitter handle to petition for an official intervention in his matter. Nakul is unable to do so because he is not internet literate, although he does also approach the Indian Embassy in Qatar

---

[30] Department of Personnel and Administrative Reforms, Government of Puducherry, Circular No.4.49011/LI2Ot7 IDPAR I CCD(2) (January 2, 2017).

[31] Kiran Bedi, Twitter, available at https://twitter.com/thekiranbedi/status/816885260575064064?lang=en (Last visited on February 20, 2019).

[32] The primary difference between States and Union Territories is that the former are administered by their own governments and the latter are governed by the Union government. However, specific Union Territories like Delhi and Puducherry do have elected governments, albeit whose powers are limited to specific subjects of governance unlike other state governments. In such cases, political power is shared and exercised by both the elected government and the Lieutenant Governor who is the direct representative of the Union Government.

requesting official help. Sahadev is an active internet user, but has not signed up to Twitter due to moral reasons relating to deficient privacy protection, and therefore, he is also forced to physically approach the Indian Embassy like Nakul for requesting help. The Minister responds to Arjun's Twitter request soon, assuring him of help and indeed the Indian Embassy in Qatar contacts him soon thereafter to discuss this matter. Both Nakul and Sahadev after several visits to the Embassy are able to finally submit their requests to the concerned officer who also assures to help out with the situation.

Situation 1 can be interpreted quite differently by different constituencies. As highlighted earlier there is an expanding group of internet users who will celebrate the use of Twitter as a platform for the Minister to reach out to Arjun. Nevertheless, should access to Twitter allow for better public service delivery? After all, Nakul, Sahadev and Arjun are all Indian citizens and, therefore, have equal rights of service from the Indian Embassy. Should internet illiteracy be an impediment to right of accessing such services? Should privacy be necessarily sacrificed to a private company, for getting the attention of the Minister? By way of analogy, we would be morally outraged if there would be an official Indian Government policy that suggests that anybody driving an expensive car or one who is English literate would get better public service response than someone who reaches the embassy by using public transport.

Such an outcome would essentially violate the moral spirit behind Article 14 ("State shall not deny to any person equality before the law or the equal protection of the laws within the territory of India") and Article 38 of the Constitution of India ("the State shall, in particular strive to minimize inequalities in income, and endeavour to eliminate inequalities in status, facilities and opportunities, not only amongst individuals but also amongst groups of people residing in different areas or engaged in different vocations.").

The Constitutional guarantee to the right to equality would at a minimum entail that all three, Nakul, Sahadev and Arjun individually would have a legitimate expectation to be treated substantially equally, given that none come from socially disadvantaged groups which would then have enabled them to argue for more privileged access to the State. Treating equals unequally primarily based on unconstitutional taxonomies such as education and access to social capital is constitutionally untenable. In addition to this, treating Arjun in a privileged manner would also amount to a perversion of the State's obligation to further the agenda of social justice by pursuing a policy to end all manifestations and practices of inequality. Such a situation would be fit case to argue that the State is pursuing an objective which is meant to actively undermine its constitutional obligation of creating the conditions for the realisation of social justice.

2. Situation 2—Communicational governance through social media

A Right to Information request reveals that the media manager at the Prime Minister's Office ('PMO') has received 20 requests for interviewing the Prime Minister of India. Out of this, the Prime Minister has responded to only 2 requests from two foreign publications (the Economist and Wall Street Journal) wherein the interview questions were shared in advance. All other requests from Indian print and television channels were refused. On the other hand, the PMO has regularly shared news and updates via Twitter and has also responded to ongoing developments like India winning cricket matches or natural calamities like destruction caused due to floods.

Situation 2 especially, brings into attention the difference between communication and transparency. Public communication by elected representatives and by the bureaucracy is not a monologue akin to periodic issuance of edicts. Communication presumes conversations between groups or individuals. Refusing requests of interviews from journalists reduces opportunities for free and fair questioning of the government and undermines democracy.[33] A dictatorial government can be very transparent about its motives and actions but not answerable to the people. Seldom do we appreciate the difference between transparency and communication, and the former does not necessarily guarantee the latter.

Further, the selection of private internet platforms for public functions bypassing due procurement processes is also ridden by problems such as confidentiality of data, charges of unjust enrichment and also adversely impacting competition. Most significantly perhaps the executive supporting initiatives such as India Stack, clearly reflects that the Aadhaar is also designed to address the delivery of private goods and services. It is, therefore, premised on the contract that provisioning and access to critical private services (like banking for instance) will require citizens to submit their biometric data and thus allow for potential surveillance.

Going forward, the State's push for Digital India and support for initiatives like India Stack and Aadhaar essentially incentivizes the accessing of public goods and services through the internet. Expanding Aadhaar for biometric authentication by private intermediaries[34] also abets the granular profiling of Indian citizens by accessing their choices and activities on the internet. This

[33] Karan Thapar, *Why Can't Modi Speak A Little Bit More To Indian Journalists?*, Hindustan Times, February 26, 2017, available at http://www.hindustantimes.com/columns/why-can-t-modi-speak-a-little-bit-more-to-indian-journalists/story-us2Fp9drMpRYRRaPGnPdlK.html (Last visited on February 20, 2019).

[34] *See*, *e.g.*, despite the clear finding by the Court in the Aadhaar judgment that Section 57 of the Aadhaar Act is unconstitutional as it allows for use of the Aadhaar system by private parties, the government has moved to circumvent this ruling by introducing an amendment to the Act through the Aadhaar and Other Laws (Amendment) Bill, 2018.

allows the State and private intermediaries to have enormous personal information about citizens. This indiscriminate collection of personal information can very well undermine the constitutional goal of a limited government and can create opportunities for abuse and resulting grave personal harm.[35]

B. STATE AND INTERNET INTERMEDIARIES

The second category worth studying would include recent attempts by both the Courts and the Executive to develop a working relationship with intermediaries[36] like private internet companies, such as Facebook, Twitter, Google as well as internet service providers (Airtel, Jio Telecom, Vodafone) in co-opting their assistance for public enforcement functions.

Under the Information Technology Act, 2000 ('IT Act'), the government can regulate a range of private conduct inter alia, offensive content, obscene material and other materials that threaten public order and sovereignty of the State.[37] The architecture of the internet is such that State has very little flexibility in adopting mechanisms for enforcing such rules. Unlike in the physical world, where it can rely on a range of sanctions and enforce them easily, with the internet, the State is forced to rely on intermediaries because first, it does not exercise complete control over activities on the internet and second, it is also difficult to keep a track of infractions of the law in the digital space. Unsurprisingly the usual response that the State has to such infractions is to either ban a particular website (for which it has to again rely on intermediaries to enforce the ban) or to shut down internet services in a particular region in the face of a law and order situation. Of course, this is an excessive response and has attracted widespread criticisms

---

[35] Ministry of Home Affairs, *supra* note 18.

[36] "Intermediary" is defined in Section 2(1) (w) of the Information and Technology Act 2000.

> "Intermediary" with respect to any particular electronic message means any person who on behalf of another person receives stores or transmits that message or provides any service with respect to that message.

[37] Under Section 79(3)(2) of the Rules framed under the amended IT Act, 2000, intermediaries must observe due diligence to see that all content that:

(a) belongs to another person and to which the user does not have any right to;
(b) is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;
(c) harm minors in any way;
(d) infringes any patent, trademark, copyright or other proprietary rights;
(e) violates any law for the time being in force;
(f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;
(g) impersonate another person;
(h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;
(i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation.

from internet users in Manipur and Kashmir, two areas which have experienced repeated shut downs.[38]

Apart from the overall regulatory framework mandated under the ITA, there are specialised legislations like the Pre-Conception and Pre-Natal Diagnostic Techniques Act, 1994 ('PC-PNDTA') which ban advertising of such services. It is difficult to enforce banning of advertising of such services on the internet without the cooperation of the intermediaries. This specific issue has also attracted the Court's attention in an ongoing litigation in *Sabu Mathew George* v. *Union of India*.[39]

In this case the Court supported the arguments of the public prosecutor mandating for positive obligations of the intermediaries (Google, Microsoft and Yahoo were the three specific respondents to this case) and held that,

"In-House Expert Body" that is directed to be constituted, if not already constituted, shall on its own understanding delete anything that violates the letter and spirit of language of Section 22 of the 1994 Act and, in case there is any doubt, they can enter into a communication with the Nodal Agency appointed by the Union of India and, thereafter, they will be guided by the suggestion of the Nodal Agency of the Union of India. Be it clarified, the present order is passed so that the respondents Nos. 3 to 5 become responsive to the Indian law."[40]

This gives us an insight into the thinking of the Executive and the Court. By delegating legal enforcement functions to the in-house expert bodies of the intermediaries, the Court is substantively expanding the legal mandate of these intermediaries to regulate content on the internet. Delegation of rule making, rule adjudication and rule enforcement powers to non-state actors is nothing new. However, the question remains on the administrative and technical capacity of public agencies to supervise such delegation. Absence of supervision may lead to abuse of this power by intermediaries and can gravely imperil freedom of speech and expression and privacy of users in the digital world.

C. CITIZENS AND INTERNET INTERMEDIARIES

The third category for our deliberation is the private contractual relationships between citizens and intermediaries. There are primarily two aspects that require careful consideration. First, whether citizens are in a position to negotiate a fair contractual relationship with intermediaries, specifically on the subject of privacy of their data and actions on the internet? Second, is the issue of whether

---

[38] *2018 is the worst year for internet shutdowns in India*, The Times of India, August 9, 2018, available at https://timesofindia.indiatimes.com/india/2018-is-the-worst-year-for-internet-shutdowns-in-india/articleshow/65333497.cms (Last visited on February 20, 2019).

[39] Sabu Mathew George v. Union of India, (2017) 7 SCC 657 : 2017 SCC Online SC 136.

[40] *Id*., ¶13.

the State has a role in intervening in this relationship, given that privacy as a territorial facet is difficult to define and achieve? Yet, the more interesting question is also whether the State would be really interested in intervening in private relations when it is invested in a project like Aadhaar? Apparently not, as is evident in the delay in the tabling of the Data Protection Bill in the Parliament despite it being ready and clear expectations of the Supreme Court as specified in the Aadhaar judgement.[41]

Further, as was alluded to earlier, consent as is practiced *inter se* between citizens and intermediaries is essentially coercive in nature because all such contracts heavily favour the service provider, since it is they who draft them. Moreover, the nature of our physical lives are such that not using certain services of private intermediaries, such as LinkedIn, is almost impossible, say for a professional looking for a white collar job. Therefore, the lack of choice also prevails upon the user rendering the consent highly extractive and reducing it to merely a formality. It is submitted that provisioning of public services and government privilege over private intermediary platforms like Twitter also creates further incentive for citizens to access such platforms and disregard the possible harm.

Flagging these three typologies is necessary not only to provide a conceptual structure to relationships on the internet in order to frame the regulatory debates relating to privacy therein, but also to underline the critical linkages between these framings,[42] for instance, the compromised position of citizens that forces them to access public officials via internet intermediaries. Amongst the three actors, State, intermediaries and citizens, it is the last category which is the most disadvantaged. These critical linkages are reflected not only in law and policy but also in explaining executive actions and judicial interventions in this context.

III. INDIAN JURISPRUDENCE ON PRIVACY

The issue of privacy has been intensely litigated right from the early days of Independence in the various High Courts and the Supreme Court of India. One of the first cases in which the Supreme Court had an opportunity to comment on the right to privacy was in the case of *M.P. Sharma* v. *Satish Chandra* ('M.P. Sharma').[43] The petitioners had challenged the constitutional validity of searches conducted on their property on the suspicion that fraud had been committed. One of the prongs of their challenge was based on Article 20(3) of the Indian Constitution that mandates "No person accused of any offence shall be compelled to be a witness against himself."

---

41 K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1 : 2018 SCC OnLine SC 1642 (Aadhaar judgment).

42 *Supra* note 22.

43 M.P. Sharma v. Satish Chandra, AIR 1954 SC 300 : 1954 SCR 1077.

The petitioner argued that the search and seizure of incriminating documents from his office premises would amount to compelling the accused to be a witness against himself. The Court did not accept this argument of the petitioner and held that the power to search and seizure is within the remit of the State, though it is regulated by law. It then went on to state that unlike under the US Constitution, the Indian Constitution lacked an analogous right to the Fourth Amendment which protected the right to privacy[44] and thus this could not be imported to interpret Article 20(3) which provides for the right against self incrimination.[45]

Despite being in the nature of an *obiter dictum*, given that it was adjudged by a Constitutional Bench (Eight judge bench), this continues to be cited as foremost statements of constitutional interpretation on the right to privacy.[46]

In the Aadhaar case, whether the right to privacy existed and whether it was a constitutional right became fundamental to the determination of the case. So in an order in the *K.S. Puttaswamy* v. *Union of India* case, [47] given on August 11, 2015, the Court found that the stakes were high as the amplitude of Article 21 was in contention. They also recognised that technically the State's argument that the larger bench *ratio* of the M.P. Sharma case was wilfully ignored by the subsequent benches and that their subsequent reiteration of the right to privacy could not overturn the applicability of the former since it was a larger bench judgement.[48]

Thereafter, the Constitutional Bench judgement[49] delivered on August 24, 2017 did uphold the right to privacy as a fundamental right under the Constitution of India. This is analyzed in detail in Section E of this part.

A. STATE SURVEILLANCE OF CRIMINAL SUSPECTS

This section discusses two important cases with similar factual backgrounds, which crystallized the right to privacy within Indian constitutional framework.

In *Kharak Singh* v. *State of U.P.*,[50] ('Kharak Singh') police surveillance of a habitual criminal was challenged as being in violation of citizen's

---

44 Cornell Law School, Legal Information Institute, *U.S. Constitution, Bill of Rights: Amendment IV (Search and Seizure).* (The Fourth Amendment of the U.S. Constitution provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.")

45 Id., ¶17.

46 *See* Mukul Rohatgi's argument against the establishment of a constitutional bench on the right to privacy, reference to which has been made in the MP Sharma case.

47 K.S. Puttaswamy v. Union of India, (2015) 8 SCC 735.

48 *Id.,* ¶¶12, 13.

49 K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 : 2017 SCC OnLine SC 996.

50 Kharak Singh v. State of U.P., AIR 1963 SC 1295.

fundamental rights guaranteed under Part III of the Constitution.[51] Two fundamental rights, namely Article 19 (1)(d) guaranteeing the right to move freely throughout the territory of India and Article 21 providing the right to life and personal liberty were specifically in contention. Surveillance by the police included several measures such as secret picketing of the house, domiciliary visits at night, verification of movements and absences.

The constitutional bench judgement was split 4:2 with the majority of the bench holding that the domiciliary visits were the only part of the regulation that violated the right to personal liberty which is recognised as a fundamental right under Article 21. Critically, the majority referred to the assurance of human dignity as one of the "concepts underlying the constitution" and these objectives of the framers have to be fully considered in construing personal liberty in a "reasonable manner." Relying on this interpretation, it held that only domiciliary visits were an invasion into the sanctity of a man's home. An intrusion into his personal security and his right to sleep, which are the normal comforts and dire necessities for human existence and, therefore, that aspect of the regulation, fell afoul of Article 21 and was struck down as unconstitutional.

The other parts of the challenge did not succeed because the majority found that the right to privacy was not a guaranteed right under the Constitution.[52] Admittedly, there was invasion of privacy but that did not amount to violation of a fundamental right as there was no fundamental right to privacy expressly provided under the Constitution of India. Domiciliary visits though were privacy invasions of a grave character and, therefore, amounted to a violation of personal liberty, as it is a compendium term and includes varieties of rights, not merely a right to continue its animal existence.[53]

The minority judgement delivered by Justice Subba Rao (on behalf of himself and Justice J.C. Shah) relied on pivotal American case law on this issue to find that all acts of surveillance under the impugned regulation infringe the fundamental rights of the petitioner under Article 21.[54] Noting that unlike in America, the Indian Constitution qualifies the term liberty with the word 'personal' and, therefore, it only relates to the liberty of the person. Appreciating that psychological restrains could be in some cases more effective than physical restraints and could engender inhibitions, therefore freedom from encroachments on private life was considered a species of the right to personal liberty and an 'essential ingredient' of the latter.[55]

---

[51] Part III of the Constitution of India enlists a number of fundamental rights which are justiciable in nature. This means that there exists a remedy in terms of challenging this violation through a legal right to move the Supreme Court or the relevant High Court.

[52] *Supra* note 50, ¶17.

[53] *Id.*, ¶14.

[54] Munn v. Illinois, (1877) 94 US 113; Bolling v Sharpe (1954) 347 US 497, 499; Wolf v Colorado (1949) 238 US 25.

[55] *Supra* note 50, ¶28.

This 'essential ingredient' argument was adopted and upheld a decade later by the three judge Supreme Court bench in *Gobind* v. *State of M.P.* ('Gobind')[56] that for the first time recognised an explicit constitutional right to privacy by interpreting Article 21 of the Constitution, albeit with many caveats. Here again the petitioner had challenged the U.P. Police Regulations which included domiciliary visits as part of larger surveillance by the police of the petitioner's activities.

The Court appreciated that with time there had come into existence new conditions including more pervasive means of invading privacy.[57] Nevertheless, it cautioned that too broad a definition of the right to privacy would be inappropriate given the absence of any explicit right to privacy in the Constitution.[58] It elucidated on a catalogue of "private" activities which was by no means exhaustive. Labelling them as "personal intimacies of home", it mentioned family, marriage, motherhood, procreation and child rearing as activities that deserve to be protected as private.[59] More importantly, any privacy-dignity claims would have to be justified as being implicit in the concept of ordered liberty. Thus apart from those catalogued by the Court, any new "private act or space" would have to be justified as necessary and essential to the protection of personal liberty under Article 21.[60]

Interestingly, the Court provided a theoretical underpinning to the importance of protecting the privacy of home. Privacy of the home ought to be protected on the ground that activities at home do not cause harm to those outside it and that home is a sanctuary away from societal control.[61] Both arguments are related of course. Sanctity of home can be justified only when the space does not result in harm to others. This is a condition precedent to right to access and inhabit a private space. Understandably, the Court contended that this fundamental right to privacy is not absolute and subject to being regulated on the ground of compelling public interest.[62]

At first glance, Gobind is not undeservedly celebrated by privacy activists, although this recognition came much later. However, the Court opted for an interpretative approach that was almost pedantic in pursuing an 'essential ingredient' argument. Perhaps a far richer exploration would have been the one suggested by the majority bench in M.P. Sharma which had sought to link privacy to human dignity and locate it in the context of constitutional morality by focusing

---

56 Gobind v. State of M.P., (1975) 2 SCC 148.
57 *Id.,* ¶23.
58 *Id.*
59 *Id.,* ¶24.
60 *Id.,* ¶24.
61 *Id.,* ¶24.
62 *Id.,* ¶28.

on values celebrated in the preamble to the Indian Constitution. I will explore this further in the fifth part of this article.[63]

This timidity perhaps stems from Court's heightened awareness of two facts—first, the absence of an explicit right to privacy in the Indian Constitution and second, the difficulty in providing for a substantive definitive content to this right to privacy. This explains the reasons behind the Court's keenness to situate the right to privacy within the ambit of an explicit fundamental right, like in this case Article 21.

B. DO PUBLIC PERSONS HAVE A RIGHT TO PRIVACY?

The balance between the public's right to know the individual's right to privacy has also been a critical area of litigation in the Indian Courts. Below, I discuss two influential cases in this regard extensively.

The first case is *R. Rajagopal* v. *State of T.N.*[64] ('Rajagopal') (commonly known as the Auto Shankar case), which dealt with the publication of a convict's autobiography and petitioner's legal action (jail officials) to stop that publication. The judgement was delivered by a two judge bench.[65]

The legal issues in this case included whether unauthorized writing of another's person's life story infringe the privacy of the concerned individual, the contour's of the freedom of press to publish such unauthorized accounts of a person's life and the remedies available to that person.

The Court recognised that the right to privacy was protected *inter se* through tort wherein the aggrieved could *post facto* bring an action for damages for violation of their right to privacy. Further, action against the State is also envisaged in cases of State invasion of privacy since it is also a constitutional right.

Following Gobind, the Court noted that the right to privacy is not one of the enumerated rights but is one of those rights which have been inferred from Article 21.[66] Freedom of press is guaranteed through the Article 19(1) freedom of speech and expression. However, it is subject to decency and defamation as specified under Article 19(2).[67] The citizenry can secure their privacy *vis-à-vis* the spaces and acts, which had also been specified in Gobind, by ensuring that nobody can publish on such subjects without their consent and it is immaterial whether the

---

[63] Gautam Bhatia, *Surveillance and the Indian Constitution - Part 2: Gobind and the Compelling State Interest Test*, The Centre for Internet & Society, January 27, 2014, available at https://cis-india.org/internet-governance/blog/surveillance-and-the-indian-consitution-part-2 (Last visited on February 2, 2019).

[64] R. Rajagopal v. State of T.N., (1994) 6 SCC 632.

[65] Justice Jeevan Reddy authored the judgment, on behalf of himself and Justice Suhas C. Sen.

[66] *Id.,* ¶9.

[67] *Id.,* ¶21.

subject matter of publication was truthful, laudatory or critical. Violations could be pursued through the filing of a tort claim for damages. However, if citizens were to voluntarily thrust themselves in a controversy then it would form an exception and they would be precluded from pursuing such a claim.[68]

Further, the Court specified that right to privacy is not available to those holding public positions (e.g. public officials) when it relates to acts and conducts relevant to the discharge of their official functions and when information is based on public record (with the exception of reporting on victims of sexual harassment, rape and other violent crimes). The Court also rejected the demand for pre-censorship as was demanded by the jail officials who had asked the Court to stop the publication on grounds of potential defamation.

Rajagopal built on the Gobind jurisprudence in significant ways. It established a moral argument recognising individual autonomy as the basis for the right to privacy. Following from this, it recognised the prerogative of an individual to exercise this right and *ipso facto* to withdraw from the exercise of this right, for instance by voluntarily thrusting herself in the public realm. More critically perhaps it distinguished between state violations of privacy which could be pursued through a constitutional challenge and violations by non-state actors which could be pursued through tort actions.[69] A continuing problem of tort actions as remedies is that it can only be used post violations largely to sue for damages and has limited impact as a tool for restorative justice or in granting injunctive relief to stop potential violations. Access to tort remedies is also governed by access to resources (both economic and social capital) which acts as an additional impediment.[70]

Significantly, the Court also expanded the list of spaces/activities which clearly fell within the private domain to include education.[71]

The second case, *Phoolan Devi* v. *Shekhar Kapoor*[72] ('Phoolan Devi') was filed to restrain an exhibition of a feature film—the Bandit Queen—based on the petitioner's life. Despite an agreement to share details of her life for the purpose of the film, the defendant found that the depiction in the film amounted to misrepresentation and violated her privacy. The defense argued that even in the absence of an agreement, the petitioner was a public figure and therefore, the defendants had the right to make the film without any reservations.

The Court accepted the defendant's contention that the petitioner was indeed a public figure going by the Black's Law Dictionary definition's that

---

68 *Id.,* ¶26.

69 *Id.,* ¶9.

70 *See* Peter W. Huber, *The Bhopalization of American Tort Law* in Hazards: Technology and Fairness (1986). (An interesting discussion of the differences between old and new tort law specifically within the American jurisdiction including the limitations of tort action suits)

71 *Supra* note 64, ¶26.

72 Phoolan Devi v. Shekhar Kapoor, 1994 SCC Online Del 788.

"public figure for right of privacy action purposes includes anyone who has arrived at a position where public attention is focused upon him as a person."[73]

However, the Court raised the question of whether being a public person would also result in a loss of right to defend when ones personal life is misrepresented or represented in a gruesome manner to highlight deeply shameful activities in the past (like in this case rape, gang rape, sexual intercourse) resulting in public humiliation without their consent.[74] The Court answered this question in the negative. The Court found that explicit display of past events in the plaintiff's life against her wishes not only caused emotional hurt and humiliation to the plaintiff but also exposed her to emotional abandonment from herself and society.[75]

As in the Rajagopal case, the Court acknowledged that consent and public record were two exceptions to the contravention of the right to privacy. The Court found that voluminous newspaper reports, periodicals and magazines relied on by the defendants could not prove that the plaintiff had unequivocally admitted to being raped, gang raped and had sexual intercourse.[76]

Further, on the issue of consent, despite entering into the agreement with the defendants, the Court found that the plaintiff had no knowledge of what was shown in the film, and despite repeated requests was not shown the entire film, and therefore, the consent given in the agreement was rendered invalid and could not be the basis for giving license to the defendants to make the film in any manner that they liked.[77]

Following from this, the Court granted an injunction restraining the defendants from further exhibiting the film abroad, since it violated the privacy of plaintiff's body and person and as exhibiting the film any further would cause further injury to the plaintiff.[78]

In this case, for the first time, there was an explicit linkage established between the right to privacy and the right to live with dignity which is recognised under the Protection of Human Rights Act, 1993. It is pertinent to note that dignity of the individual is mentioned within the definition of 'human right' in the Act, however, the right to privacy is not explicitly recognised within the Act.[79] Further, the definition of 'human rights' does refer to rights embodied in International Covenants and enforced by Courts in India. Article 17 of the

---

[73] *Id.,* ¶31.
[74] *Id.,* ¶34.
[75] *Id.*
[76] *Id.,* ¶40.
[77] *Id.,* ¶41.
[78] *Id.,* ¶45.
[79] Article 17(1) of the International Covenant on Civil and Political Rights, 1966 states that, "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."

International Covenant on Civil and Political Rights expressly recognises the right to privacy and therefore, is made applicable through the domestic legislation in India.

Thus, despite consent being expressly provided, it cannot be stretched and abused to undertake actions that violate the dignity of the consent-giver. Thus consent *per se* is not a defence or justification for actions which abuse that consent. Logically speaking, this also reflects the fair expectation that consent can only be exercised for benefit and at least when *no harm* results from the exercise of such a choice. The individual has complete autonomy in the manner in which their thoughts, sentiments and emotions are publicly communicated. Resultantly, even a public person retains a certain degree of autonomy to the extent that it protects a fair expectation that consenting to sharing of privacy would not result in personal harm.

This principle of no harm is of import in the context of the internet. In most times, formal consent or even tacit consent is considered to be adequate in providing legitimacy and or legality to activities online. However, this exercise of consent should also be accompanied by the principle of no harm should result from this consent. This would provide an obligation on the consent taker to ensure no harm results and much beyond the current practices of due diligence obligation under the IT Act.

C. PRIVACY VIOLATIONS BETWEEN PRIVATE PERSONS

Privacy violations can happen *inter se* between private persons. The problem though arises in the context of remedies.

Despite the clear distinction that Gobind made between tort and constitutional remedies in case of privacy violations by non-state actors and the State respectively, the limitations of the tort remedy have meant that constitutional remedies continued to remain relatively more attractive to pursue violations of privacy *inter se*.[80] Procedural and substantive impediments to accessing constitutional remedies to pursue privacy violations *inter se* have posed a challenge. This section discusses three cases, wherein this issue came to the fore.

People's Union for Civil Liberties v. *Union of India*[81] ('PUCL') was concerned with the unauthorised snooping or interception of phone conversations between private individuals. Phone tapping was undertaken in an unauthorised manner by MTNL (a government public sector undertaking) at the oral requests of representatives of competent authorities.

[80] Constitutional remedies like writs have continued to be used by persons to pursue violations between private parties as is evident from petitions such as one filed by Karmanya Sareen against WhatsApp discussed in this section.

[81] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.

The Court accepted that every government (even democratic ones) would tap phones as part of intelligence gathering. However, citizen's right to privacy had to be protected against abuse by authorities.[82]

The statutory framework for this purpose is governed by the Indian Telegraph Act 1885. The Court noted that the Act lays down the purposes[83] for which interception of telephones could be permitted. However, the Central Government had made no Rules on this issue. Further, it was provided that the procedure for intercepting of phones should be just, fair and reasonable.

The Court relied on the cases of Kharak Singh, Gobind and Rajagopal to hold that telephone tapping violated not only the right to privacy (which was an interpretation of Article 21) but also Article 19(1)(a) which guarantees the freedom of speech and expression.[84] It also quoted Article 17 of the International Covenant on Civil and Political Rights, 1966 and Article 12 of the Universal Declaration of Human Rights.[85] Most importantly, the Court sought to explicitly link Article 21 with the international law covenants by arguing that Article 17 of the International Covenant on Civil and Political Rights was not in conflict with municipal law and therefore, the latter should be interpreted in conformity with international law.[86]

Underlining that it is difficult to provide for an exhaustive content to the right to privacy, it was determined that consideration would depend on the facts of the case and the burden squarely lay in the claimant to prove that the right would be attracted in the particular facts of their case.[87]

It is overwhelmingly apparent from this discussion that both the presence of the statutory framework along with the Court's attention to procedure would mean that phone interception undertaken by private non-state actors would be illegal.

The Court seems to have been mindful of this scenario when it quoted the Second Press Commission Report stating that telephone conversations

---

82 *Id*., ¶1. The judgment was delivered by a two judge bench of the Supreme Court, with Justice Kuldip Singh delivering the judgment also on behalf of Justice S. Saghir Ahmed.

83 Section 5 of the Indian Telegraph Act provides that in the event of a public emergency and in the interest of public safety, the Central and State governments can intercept messages if it is satisfied that it is necessary and expedient to do so in the interest of sovereignty and integrity of India, security of the State, friendly relations with foreign state, public order and preventing incitement to the commission of an offence.

84 *Id.,* ¶19.

85 Reference was made to the minority opinion of Justice Khanna in ADM, Jabalpur v. Shivakant Shukla, (1976) 2 SCC 521, wherein he had discussed a well establish rule of statutory interpretation, i.e. in case of conflict between municipal law provisions and international law provisions, the former will prevail. However, if two constructions of municipal law provisions are permissible, Courts will lean on that construction which will allow for harmony between the two.

86 *Supra* note 81, ¶26.

87 *Id.,* ¶18.

are of intimate and confidential nature and therefore, tapping results in a serious violation of privacy. Since there was no general right to privacy under law, therefore, tapping could not be regarded as a tort.[88]

Given that post liberalization there has been a rapid expansion of private telephone service providers (both mobile telephone and fixed land lines) what would be the remedies available to private citizens if such telephone interception were to be carried out by private telecom service providers? More interesting, perhaps, is what would be the remedies available for such violations in the digital space? Will tort remedies suffice especially when consent through contractual means (however one sided) would be used as a defense in such matters? Very unlikely, would be the short answer.

In this context, the pedantic distinctions between public harms addressed through public law remedies (like Article 32 writ petitions requesting the intervention of the Supreme Court to address violations of fundamental rights) and private harms that are to be addressed through torts are ostensibly not very helpful.

The second case in this respect is *Indu Jain* v. *Forbes Incorporated*,[89] wherein Indu Jain[90] sued Forbes Magazine for a news article and requested for an interim injunction from the Delhi High Court prohibiting the publication of the news report on the defendant, since it was a breach of her right to privacy. Justice Gita Mittal who heard the case undertook a detailed discussion of the right to privacy, especially in the context of remedies available for its violation.

It is interesting to note that despite coming nearly a decade post Rajagopal, the petitioners chose not file it as a writ petition, based on the violation of their constitutional right to privacy, but in fact framed this petition to secure public safety, individual security and privacy of the petitioners. In hindsight, this proved to be a sound choice.

The petitioner's arguments were based on the infringement of her right to privacy, which is an implicit right under Article 21 (right to life and personal liberty) of the Constitution of India. Publication of the petitioner's financial wealth was within the realm of privacy and publishing on the matter without her consent violated that right.[91] Although as a shareholder of the Bennett Coleman & Co, she was a paid employee, she had no other connection as to the day to

---

88 *Id.,* ¶32.

89 Indu Jain v. Forbes Incorporated, 2007 SCC Online Del 1424.

90 Indu Jain at that time was one of the major shareholders of the proprietary firm Bennett and Coleman, a media organisation in India whose newspapers include The Times of India, which is the largest circulated English newspaper in India. This is important because as per the previous standards established by Rajagopal, she could be referred to as a "public person", given her role as a business titan.

91 *Supra* note 89, ¶33.

day functioning of the company and therefore, could not be identified with the same.[92] Publication of the private information impacted her security in a concerning manner.[93]

The defendant's counsel, Soli Sorabjee contested the claim that the right to privacy judicially deduced from Article 21 was enforceable against the State and in this case since the defendants were private individuals, the claim was not enforceable against them.[94] It was argued that the right is not absolute, and given that the petitioner is a public person, had waived their right to privacy.[95] Further, it was submitted that mentioning a person's wealth or income is not an invasion of privacy and such information cannot be entitled to protection.[96]

Justice Mittal framed the following legal issues.[97] Was the right to privacy part of the fundamental freedoms guaranteed under Article 21 of the Constitution? Was this fundamental right enforceable against another private person i.e. would it have horizontal application? Was the right to privacy was recognized as a tort? What is the balance to be struck between freedom of press and the right to privacy, especially if it concerns a public person? Can interim reliefs like injunction be granted to prohibit publication?

Justice Mittal referred to the well established jurisprudence in Kharak Singh, Gobind and Rajagopal cases and found that although the right to privacy is not expressly guaranteed under the Constitution of India, through judicial interpretation Article 21 has been said to include this right.[98]

When deciding the question as to whether constitutional remedy is available for privacy violations *inter se*, the Court relied on *P.D. Shamdasani* v. *Central Bank of India Ltd.*[99] *and Vidya Verma* v. *Shiv Narain Verma*[100] to reason that, horizontal application of fundamental right cannot be presumed unless expressly provided enumerated in the Constitution and therefore, fundamental rights are primarily enforceable against the State.[101] However, it was pointed out that the Constitutional scheme does expressly provide for horizontal application under Articles 17, 23 and 24.[102]

---

92 *Id.,* ¶33.
93 *Id.*
94 *Id.,* ¶35.
95 *Id.,* ¶¶34, 35.
96 *Id.,* ¶36.
97 *Id.,* ¶40.
98 *Id.,* ¶¶41, 42, 43.
99 P.D. Shamdasani v. Central Bank of India Ltd., AIR 1952 SC 59 : 1952 SCR 391.
100 Vidya Verma v. Shiv Narain Verma, AIR 1956 SC 108.
101 *Supra* note 89, ¶51.
102 *Id.,* ¶¶52, 53. Reference was made to the decisions of the Supreme Court in Zoroastrian Coop. Housing Society Ltd. v. Registrar, Coop. Societies (Urban), (2005) 5 SCC 632 and People's Union for Democratic Rights v. Union of India, (1982) 3 SCC 235.

The Court in an earlier case[103] had held that Article 21 is not enforceable against private persons. Merely because the Constitution provides for enforcement of certain fundamental rights against private parties, it would not extend such application to Article 21 also.

On the issue whether the right to privacy is recognised as a tort in India, Justice Mittal did not provide a conclusive answer. She only referred to Rajagopal to quote that the unlawful invasion of privacy could be protected as a tort and as a constitutional right and noted that the former is not statutorily protected in India.

Relying on American jurisprudence, she reasoned that freedom of press *vis-à-vis* the right to privacy requires a balancing of interests. Primacy will be given to the freedom of press especially when the person concerned is a public person and therefore, the public has a rightful interest or whether information is for the public benefit.[104] Right to privacy can also be waived by consent and such a waiver can be express or by tacit consent.[105]

Following the judgement in *S. Rangarajan* v. *P. Jagjivan Ram,*[106] the Court noted that the freedom of press should not be suppressed unless the situation created by allowing the freedom are pressing and community interest is endangered.[107] The Court discussed the difficulties in clearly sequestering the privacy from the public life of individuals and referred to the reasonable person standard in judging whether what conduct or information would take form of private's person life.[108]

Referring to *Ajay Goswami* v. *Union of India,*[109] the Court reiterated that the test of privacy violation is that of the sensibilities of an ordinary man of common sense and prudence and not an out of ordinary or hypersensitive man.[110] Applying this test to the facts of this case, the Court noted that the petitioner had admitted that she is a public person and that this was widely acknowledged in the media and in such a circumstance it was not an option for the petitioner to claim seclusion.[111]

Interestingly, the Court referred to *Bret Michaels* v. *Internet Entertainment Group Inc.*[112] on what is considered "newsworthiness". It was held that it not only includes matters of public concern but also accomplishments,

---

[103] Bijayalaxmi Tripathy v. Managing Committee of Working Women's Hostel, 1992 SCC OnLine Ori 43.
[104] *Supra* note 89*,* ¶71.
[105] *Id.,* ¶84.
[106] S. Rangarajan v. P. Jagjivan Ram, (1989) 2 SCC 574.
[107] *Supra* note 89, ¶159.
[108] *Id.,* ¶160.
[109] Ajay Goswami v. Union of India, (2007) 1 SCC 143.
[110] *Supra* note 89, ¶152.
[111] *Id.,* ¶226.
[112] Bret Michaels v. Internet Entertainment Group Inc*,* Lexsee 5 F Supp. 2d 823.

everyday lives and humanity involvements of famous persons. This is to be construed along with the caveat, that if the publicity is so offensive as to constitute a sensational prying of the private lives or its own sake and serves no legitimate public interest, then it is not deserving of protection.[113] This is of course an emanation of the reasonable person test. As with all reasonable person tests, this too is largely dependent on the facts of each case, which are framed by the judge, and the proclivities of the judge herself.

The petitioner's counsel had argued that matters relating to finances would be covered under, "among other matters" under Rajagopal. This was challenged by Soli Sorabjee who argued that finances of a corporation or a corporate group would be excluded from the ambit of such personal matters. Responding to this, the Court found that first, the petitioner herself had voluntarily provided material and information relied on by the defendant to publish the article.[114] Further, the news report was in the nature of a economic analysis of public data i.e. material freely available in the public domain and thus concluded that the information and details which was the basis for the news report was neither private nor secret.[115]

Furthermore, the Court extracted from the written communications exchanged between the petitioner and the defendant to ultimately deduce consent for the publication to publish.[116]

Finally, considering the prayer of interlocutory injunction, the Court relied on *Shree Maheshwar Hydel Power Corpn. Ltd.* v. *Chitroopa Palit*[117] to contend that unlike its English counterparts, Courts in India were entitled to scrutinize whether statements made in the publication were *bona fide* and in the public interest and that the defendants had undertaken due diligence to ascertain the truth.[118] The Court found that the communication, the methodology and the public information gathered made it clear that the defendants did fulfil this burden of due diligence.[119] The prayer for interlocutory injunction also failed because the petitioner had given implicit consent for the publication. It was thus well settled, that with consent even matters which are in the private domain can be made public.[120]

Ultimately the Court relied on implied consent provided by the petitioner, along with the public interest nature of the publication itself to deny the prayer.[121] This case is interesting not only because it addressed for the first time the important question of whether constitutional remedies could address privacy violations *inter se,* but also because of the extensive account of the various principles

[113] *Supra* note 89*,* ¶145.
[114] *Id.,* ¶189.
[115] *Id.,* ¶192.
[116] *Id.,* ¶201.
[117] Shree Maheshwar Hydel Power Corpn. Ltd. v. Chitroopa Palit, 2003 SCC OnLine Bom 702 : AIR 2004 Bom 143.
[118] *Supra* note 89, ¶165.
[119] *Id.,* ¶¶166, 193.
[120] *Id.,* ¶¶189, 213.
[121] *Id.,* ¶237.

guiding the application of the right to privacy. Despite such a clear exposition of the legal position, new petitions continued to be filed claiming the application of constitutional remedies to such violations *inter se.*

As we see in the next case, this claim emanates from two very practical considerations. First, that privacy violation if they were to be addressed through writ jurisdiction of the Court would allow petitioners faster access to appellate courts and therefore possibly faster relief. Second, given that the right to privacy lacks complete definition, as has been reiterated in Gobind, Rajagopal and PUCL cases, it allows the petitioners greater flexibility in constructing claims based on the constitutional idea of privacy rather than rely on tort claims.

It is hard to logically justify that violations of the right to privacy will be treated differently based on the nature of the violator. Despite clear textual basis in the Constitution, until the remedies are equally competitive in terms of access, claimants will always be incentivized to take recourse to the easier remedy despite clear statements by the Courts to the contrary. This proclivity is further exacerbated in the digital space where the State itself plays an important role as an intervener in purely *inter se* relationships as well.

The third case in this context is *Karmanya Singh Sareen* v. *Union of India*,[122] which challenged the change in the privacy policy of WhatsApp post their takeover by Facebook in 2014.

The case was first filed in the Delhi High Court. The two judge bench (Justice Rohini and Justice Sangita Dhingra Sehgal) allowed the filing of the public interest litigation despite it being vehemently opposed on grounds that this was a contractual matter strictly between two private parties.

Counsel for the petitioner, however, argued that the proposed change in the privacy policy of WhatsApp (relating to data of users of WhatsApp) would infringe their fundamental right to privacy guaranteed under Article 21 of the Constitution of India.

Arguments were also based on the faulty consent mechanism and the information given by WhatsApp to users as to the effect of this change.[123] User's arguably had proprietary ownership of the data (including identification of the users themselves as well as the content generated through messaging) and *ipso facto* WhatsApp was merely a service provider with no right of ownership of this data.[124] Consent taken by WhatsApp for the new privacy policy was also questioned on the ground that most users lacked adequate comprehension of the provisions and consequently it was not informed consent.[125] More interestingly, given that it had initially attracted users primarily based on the promise of their end-to-end

[122] Karmanya Singh Sareen v. Union of India, 2016 SCC Online Del 5334.
[123] *Id.,* ¶4.
[124] *Id.,* ¶ *Id.,* ¶2 (Subsection (d) of prayers).
[125] *Id.,* ¶6.

encryption and heightened privacy policy, it was said that WhatsApp should thereafter be estopped from withdrawing or diluting the said policy.[126]

The Court reasoned that since the authoritative determination of the right to privacy in the Indian constitution had been referred to a Constitutional bench of the Supreme Court in *K.S. Puttaswamy* v. *Union of India*,[127] the right itself cannot be a valid ground to grant relief.[128]

Moreover, the Court also noted that the Terms of Service of WhatsApp were in the nature of a private contract and not governed by any statutory provision and thereby not amenable to the writ jurisdiction under Article 226 of the Constitution of India.[129]

Despite denying substantive jurisdiction in this matter, the Court directed WhatsApp to completely delete all data of users who had opted out from their servers.[130] For other users, their data prior to the coming into effect of the new policy (25.09.2016) was instructed to be not shared with Facebook.[131] The Court also directed TRAI (Telecom Regulatory Authority of India) and the Department of Telecom to consider the feasibility of bringing such internet messaging applications such as WhatsApp under the statutory regulatory framework.[132]

Given that the High Court has a wider ambit in terms of its power to issue writs than the Supreme Court, its refusal to exercise its jurisdiction in this case, is interesting. One can conjecture that although the Court did appreciate the weight of evidence that the revised privacy policy of WhatsApp would have a material impact on the privacy of the user, it seemed to have been unconvinced as to whether a constitutional remedy would be available for such redress, especially when the right to privacy, forming the basis of such a claim, had yet to have its constitutional status determined by the Supreme Court at the time. This may also explain why the Court provided some relief to the petitioners.

The petitioners in this case have filed a petition challenging this decision in the Supreme Court.[133] Despite both WhatsApp and Facebook challenging the maintainability of the suit given that this is squarely a contractual matter and therefore not within the writ jurisdiction of the Supreme Court, the Court has allowed the filing of the matter and has referred it to a 5 judge constitutional bench.[134]

---

126 *Id.,* ¶5.

127 K.S. Puttaswamy v. Union of India, (2015) 8 SCC 735.

128 *Supra* note 122, ¶17.

129 *Id.,* ¶18. Article 226 in fact is of a wider remit that Article 32 since it allows the High Court to take cognizance of "any other matter".

130 *Supra* note 122, ¶20 (Specifically (i)).

131 *Id.* (Specifically (ii)).

132 *Id.* (Specifically (iii)).

133 Karmanya Singh Sareen v. Union of India, S.L.P.(C) No. 804 of 2017.

134 *SC Forms Constitution Bench to Hear the WhatsApp Case*, LiveLaw, April 18, 2017, available at https://www.livelaw.in/sc-forms-constitution-bench-hear-whatsapp-case/ (Last visited on February 20, 2019).

Interestingly, Mr. Harish Salve, the counsel for the petitioner argued for the maintainability of the suit, on the ground that the policy formulated was unacceptable as it affects individual freedom, which is a fundamental right under the Constitution.[135]

The adjudication on the petition is still underway and with the clear reaffirmation of the fundamental right to privacy, it is expected to be a test case of whether this right has *inter se* application. More specifically, it is likely to be an indicator as to whether the positive obligation of the State is exhausted or at least legally satisfied with the enactment of a Data Protection Act. In such circumstances, one can presume that this statutory framework will regulate such *inter se* relationships between data collectors and those users whose personal data is being collected. At the very least one can conjecture that post the entry into force of the new Data Protection Act, the legal obligations on intermediaries like Facebook and WhatsApp will be relatively more stringent than under present circumstances.

D. WHAT IS PRIVATE?

It is difficult to define the nature and scope of private actions and spaces especially in the context of our digital lives. In this section I will attempt to provide an overview of the legal conceptualizations of the idea of privacy, drawn primarily from Indian jurisprudence and specifically discuss its implications in the context of the digital world..

Both M.P. Sharma and Kharak Singh sought to secure the privacy of the home. It was therefore, the residential space and the presumption that this space should be left untouched by unwarranted interruptions and interventions specifically by the State that was emphasised. Evidently therefore, this right is not absolute. Intervention can be warranted by the State in case this space is used for public harm, as in the case of criminal activities.

There are two aspects that are worth commenting on. Perhaps aware of the tenuousness of the constitutional basis of the right to privacy, Court was reluctant to elucidate on the nature and scope of this right. However, this reluctance to enumerate could also be driven by a greater (but quiet) appreciation of the right of autonomy of the individual to use this private to commit or not commit activities, the determination of which was solely left to that individual. This may explain the Court's focus on residence as a private space rather than on specific private activities. The idea of the residence space or home itself is interesting because it alludes to a physical space that is bounded and not visible or accessible to the "other". Permission for entry is required from those that inhabit this space.[136]

---

[135] Karmanya Singh Sareen v. Union of India, (2017) 10 SCC 638 : 2017 SCC Online SC 434, ¶4.

[136] *See* Bert-Jaap Koops & Masa Galic, *Conceptualising space and place: Lessons from geography for the debate on privacy in public* in PRIVACY IN PUBLIC SPACE: CONCEPTUAL AND REGULATORY

Gobind, first attempted an enumeration of certain activities as private, with the caveat that this was not an exhaustive list. It listed "personal intimacies of home" i.e. family, marriage, motherhood, procreation and child rearing as activities that are firmly within the private realm and deserving of legal protection. The PUCL case was important in expanding this list to include telephone conversations as also private.

Since then there have been various cases, in which the Court has supported the spousal right to privacy not only in their matrimonial home but also in matters of dissolution of marriage, as a basis for rejecting or dismissing applications by third parties on this issue.[137] The right to privacy has also been litigated vigorously in matrimonial disputes specifically in the context of use of DNA testing to establish paternity of children.[138] Involuntary taking of DNA samples would violate the privacy of the individual, and the Court has advised consideration of this aspect and therefore established the obligation of establishing eminent need in such contexts.[139]

Right to privacy of the body has also been litigated vis-à-vis the use of criminal investigation technologies like Polygraph test (Lie Detector), BEAP (Brain Electrical Activation) test and Narco analysis. *Selvi* v. *State of Karnataka*,[140] is the landmark case. The Court began by reiterating that the right to privacy has been recognized as a constitutional right as an emanation of Article 21 and Article 19, however, it could be justifiably curtailed if it was done in light of competing interests. Additionally, reference was made to Article 20(3) which is right against self incrimination for criminal cases. The Court propounded a theory of interrelationship between Article 21 and Article 20(3) and the sections of the Evidence Act that establishes the rule against involuntary concessions.[141] It "conjunctively read" all three to hold that an individual decision to speak or to remain silent reflects individual autonomy of choice and to subject the individual to these techniques is to violate the bounds of privacy and would therefore come into conflict with the right against self incrimination.[142]

The Court took cognizance of the fact that the applicability of Article 20(3) is limited to criminal cases and also undertook an extensive review of the use of such techniques in civil matters by expanding substantive due process requirements of ensuring that measures undertaken to limit civil liberties embedded

---

CHALLENGES (Tjerk Timan, Bryce Newell, & Bert-Jaap Koops ed.) 19-46 (2017). (For an excellent discussion on the conceptualization of space).

137 Baldev Singh v. Surinder Mohan Sharma, (2003) 1 SCC 34.

138 *See*, *e.g.*, Narayan Dutt Tiwari v. Rohit Shekhar, (2012) 12 SCC 554; P.S. Shivakumar v. P.H. Subbarayappa, 2017 SCC OnLine Kar 2263; Dipanwita Roy v. Ronobroto Roy (2015) 1 SCC 365; Nandlal Wasudeo Badwaik v. Lata Nandlal Badwaik, (2014) 2 SCC 576.

139 Bhabani Prasad Jena v. Orissa State Commission for Women, (2010) 8 SCC 633.

140 Selvi v. State of Karnataka, (2010) 7 SCC 263.

141 *Id*., ¶100.

142 *Id.,* ¶¶ 225, 226.

under Article 21[143], safeguard the right to fair trial[144] and the rights against cruel, inhuman or degrading treatment.[145]

Interestingly, the Court commented on the contours of the idea of "*compelling* state interest". While accepting that it is primarily the Legislature's responsibility to balance the competing interests of personal liberty and public safety, it underlined that the forcible administration of such techniques could lead to a slippery slope in incentivizing police officers to rely on such techniques rather than proceed by way of scrupulous investigation.[146]

Ultimately the Court held that forcible administration of these techniques not only violates the right to self incrimination but would also violate "substantive due process" which is required for restraining personal liberty, as it would be an intrusion into the mental privacy of an individual.[147] Furthermore, this would also amount to cruel, inhuman or degrading treatment and was therefore a violation of international human rights norms and compromise the right to fair trial.[148] Finally, it was stated that invocations of compelling public interest could not justify dilution of constitutional rights such as the right against self incrimination.[149]

The Court allowed for voluntary administration of the impugned tests, but prohibited the admission of such test results as evidence. These results were given the status of claims by the accused and were subject to the review as under Section 27 of the Indian Evidence Act, 1872.[150]

Search and seizure by the police have continued to feature prominently involving arguments on privacy. The Court in *District Registrar and Collector* v. *Canara Bank* [151] *relied on Gobind* to reiterate that the right to privacy was an emanation of the fundamental rights (Articles 19(1)(a) and (d) and 21) and, although not absolute, that State intrusion can be a reasonable restriction only if it has a reasonable basis or reasonable materials to support it. The Court in this case held that privacy relates to people and not places,[152] and following from that, documents of the customer which are in the bank must continue to remain confidential,

[143] Reliance was placed on Maneka Gandhi v. Union of India, (1978) 1 SCC 248 and Rustom Cavasjee Cooper v. Union of India, (1970) 1 SCC 248 positing that what is punitively outrageous, scandilisingly unusual or cruel and rehabilitatively counterproductive, is arguably unreasonable and arbitrary and is shot down by Articles 14 and 19 and if inflicted with procedural unfairness, falls foul of Article 21.

[144] D.K. Basu v. State of W.B., (1997) 1 SCC 416

[145] *Supra* note 140, ¶¶239-242, 245.

[146] *Id.,* ¶258.

[147] *Id.,* ¶¶248, 263.

[148] *Id.,* ¶ 263.

[149] *Id.,* ¶261.

[150] *Id.,* ¶264.

[151] District Registrar and Collector v. Canara Bank, (2005) 1 SCC 496.

[152] Detailed discussion alluded to US case law relating to rejection of the Miller test (United States v. Miller, (1976) 425 US 435) and upholding the ratio in Katz v. United States, ((1967) 389 US 347) that the protection of privacy relates to people and not to places.

even if that is not in the customer's house and have been voluntarily shared with the bank. The Collector cannot violate the privacy of the customer by seizing this document unless there is a reasonable cause or basis for the collector forming the opinion that the documents will lead to discovery of any fraud or omission.[153] It found that the Andhra Pradesh Amendment Act (17 of 1986) (section 73) to the Indian Stamps Act 1899, allowed unfettered powers to the Collector to access documents which were in the private custody and were found to be violating privacy of both the house and the person and was therefore found to be *ultra vires* of the constitution.[154]

Similarly, in *Directorate of Revenue* v. *Mohd. Nisar Holia*[155] the Court considered the search and seizure powers under the Narcotic Drugs and Psychotropic Substances Act, 1985. The Court reiterated that right to privacy relates to persons and not places and therefore, although a hotel was a public place, a guest was entitled to privacy in his room at the hotel.[156] It also held that the State cannot be given untrammelled power to infringe the right to privacy of any person unless that power is governed by reasonable restrictions, for instance, the requirement of establishing probable cause for search before a magistrate.[157]

Similarly, in *Manashi Sinha* v. *State of W.B.*[158] the Calcutta High Court held that the midnight raid in the house of a decent family with no criminal antecedents is an affront to the privacy of the members of the family and also their human rights and degrades the concept of dignified life under Article 21 of the Constitution.[159]

The Court has also sought to frame acts of sexual violence and rape as unlawful intrusion into the right of privacy[160] and sanctity of a woman. Such reframing has also helped in expanding State responsibility for survivors of such sexual violence in terms of access to medical procedures and other health treatments and in ensuring their safety and guard against any arbitrary and unlawful interference with their privacy.[161]

Privacy as a right to self determination in terms of autonomy of choice was adjudicated upon in *Anuj Garg* v. *Hotel Assn. of India*[162] *ultimately upholding the right to choose their employment. In this case, the Court also stated*

---

153 *Supra* note 151, ¶58.

154 *Id.,* ¶60.

155 Directorate of Revenue v. Mohd. Nisar Holia, (2008) 2 SCC 370.

156 *Id.,* ¶14.

157 *Id.*

158 Manashi Sinha v. State of W.B., 2004 SCC Online Cal 485.

159 *Id.,* ¶ 40.

160 *See, e.g.*, State of Punjab v. Ramdev Singh, (2004) 1 SCC 421 and Lillu v. State of Haryana, (2013) 14 SCC 643.

161 *See, e.g.,* Geetanjali Gangoli & Martin Rew, *Continuities and Change: The Law Commission and Sexual Violence*, 6 JILS 108 (2014-15).

162 Anuj Garg v. Hotel Assn. of India, (2008) 3 SCC 1.

that the State protection granted to ensure security of women should not translate into censorship. The Court held that personal autonomy includes both the negative right of not to be subject to interference by others and the positive right of individuals to make decisions about their life, to express themselves and to choose which activities to take part in.[163] *Self-determination of gender is an integral part of personal autonomy and self-expression and falls within the realm of personal liberty guaranteed under Article 21 of the Constitution of India.*[164]

As is evident from the discussion in this section, there is acceptance and reiteration by Indian courts of the Katz v. *United States*[165] doctrine that privacy inheres in the person and not the physical space they inhabit opened up new ways of thinking about the right to privacy. Both the physical and mental aspects of privacy have been recognised and protected by the Courts. Privacy in public spaces including online or in the digital space should be protected. This provides us the moral ground to question indiscriminate surveillance online by intermediaries and the Government (consider for instance the proposal for a social media hub)[166] and of physical spaces (such as CCTV cameras installed by private security agencies and the police).

Courts have repeatedly censured over-delegation and unlimited powers of search and seizure to the executive without probable cause and without due supervision by judicial authorities so as to limit procedural abuse. This same standard needs to be applied for activities online of which a substantial part is analogous to private communication like phone conversations and written communication through the post. Autonomy of choice has also been upheld to curb the State action in deploying censorship as legitimate means for addressing issues of potential harm.

The conceptualization of consent as something intrinsically connected with the expectation of *no harm* is also an important principle. This destabilises the straitjacket idea that consent should be the only formal prism to justify even highly unequal and harmful relationships. The idea of consent is of course an expression of autonomy. However, circumstances under which consent is given and the potential harm which may result from that consent, provide a moral ground for not relying on formal consent as a category for legitimizing deeply unequal and flawed relationships that require the taking of personal data from an unwilling or

---

[163] *Id.,* ¶¶34, 35.

[164] There have been other cases where right to privacy has been litigated specifically in the compulsory taking of DNA information, such as in Bhabani Prasad Jena v. Orissa State Commission for Women, (2010) 8 SCC 633 and in the context of the usage of narco analysis in criminal trials such as in Selvi v. State of Karnataka, (2010) 7 SCC 263.

[165] Katz v. United States, (1967) 389 US 347.

[166] *See, e.g.*, Kumar Sambhav, *Govt. Was Watching Citizens' Social Media Accounts Since 2016*, Business Standard, December 9, 2018, available at https://www.business-standard.com/article/current-affairs/govt-monitoring-social-media-accounts-of-citizens-since-2016-reveals-rti-118120500372_1.html (Last visited on February 20, 2019).

more pertinently unknowing (in terms of the potential harm that can result from takings of personal data) individual.

E. RIGHT TO PRIVACY AS A FUNDAMENTAL RIGHT

A nine judge Constitutional Bench of the Supreme Court was established in July 2017 to consider whether there was a fundamental right to privacy under the Constitution of India. The judgement of the Court was pronounced on 24th August 2017.[167] The final judgement includes six separate opinions.[168] It is necessary to discuss the six opinions because the final order of the Court itself was limited to the pronouncement that the right to privacy was an intrinsic part of the right to life and personal liberty under Article 21 and could also be drawn from the other freedoms granted under Part III of the Constitution of India.[169]

The opinion authored by Justice D.Y. Chandrachud reaffirmed Gobind, PUCL and Rajagopal rulings (amongst others) to uphold that the right to privacy was indeed a fundamental right and that it straddled several fundamental rights recognized under Articles 15, 19, 21 and 20(3).[170] He found that the right to privacy, like other fundamental rights, is primordial and therefore a natural right.[171] Although like any other fundamental right this too is not absolute and subject to reasonable restrictions by the State.[172] Most instructively, Justice Chandrachud referred to the rapid expansion of the internet and social media to reason that sticking to an originalist interpretation of the Constitution would defeat the purpose of upholding fundamental rights in contemporary India.[173] It was noted that in the informational age challenges to privacy emanate both from State action and non-State entities, wherein the increasing uses of big data analytics would render consent and non-discrimination difficult.[174]

In terms of the standard of review adopted by the Court to assess the constitutional compatibility of restrictions imposed on the right to privacy, the Court adopted the Article 21 standard that first, there should be a law allowing for the restriction, second, that the said law is reasonable (Article 14 test) and third, that the measure effected was proportional to the aims that it seeks to achieve.[175] Interestingly, the right to privacy has both negative and positive aspects in terms

---

[167] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1. References are made to the judgment as provided on the website of the Supreme Court of India in K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

[168] Justice D.Y. Chandrachud (on behalf of R.K. Agrawal, Nazeer, Kehar and himself); Justice Chelameswar, Justice Bobde, Justice Rohington, Justice A,M. Sapre and Justice Sanjay Kishen Kaul.

[169] *Supra* note 167, Justice Chandrachud, ¶2.

[170] *Id.,* Part T (Our Conclusions), ¶3(C).

[171] *Id.,* Part G (Natural and inalienable rights), ¶40.

[172] *Id.,* Part S (Informational privacy), ¶183.

[173] *Id.,* Part M (Constituent Assembly and privacy: limits of originalist interpretation), ¶149.

[174] *Id.,* Part S (Informational privacy), ¶¶173, 174.

[175] *Id.,* Part Q (Substantive Due Process), ¶165.

of determining the obligations of the State.[176] The negative aspect is that it acts as a restraint on the State and the positive aspect is that it obligates the State to take all necessary measures to protect privacy of individuals, including through a robust data protection regime. It was also added that the State has to carefully balance the protection of privacy (of an individual) with that of legitimate State interest.[177]

Justice Chelameswar's opinion echoed Justice Chandrachud's in highlighting that privacy claims may arise against both State and non-State actors.[178] He also rejected originalist interpretations of the Constitution, instead arguing that the Constitution was a testament created to securing the goals mentioned in the Preamble and that Part III was incorporated to achieve those objectives provided under the Preamble.[179] In terms of standard of review, the opinion differentiated between species of privacy interests/claims and provided that the strict scrutiny test would only be attracted for certain kinds of privacy claims.[180] The strict scrutiny test involves review of the concerned state measure (which is challenged as violating the fundamental freedoms) on the basis that the objective qualifies as compelling State interest and the requirement that it was narrowly tailored to meet those objectives. This presumes a hierarchy amongst privacy claims to be judicially determined.

Justice Bobde departs from Justice Chandrachud's judgment in one significant way. He clearly differentiates between right to privacy as a fundamental right with reference to restrictions imposed by the State and as a common law right *vis-à-vis inter se* violations.[181] Thus, for privacy violations between private legal persons, the remedy available would only be that a common law right to sue as a tort violation would be available. This would of course greatly negate any gains received from recognizing it as a fundamental right under the Constitution of India. However, along with Justice Chandrachud and Justice Chelameswar, Justice Bobde locates the philosophical basis of the right to privacy as an inalienable natural that seeks to protect the dignity and autonomy of the individual.[182]

Justice Nariman also echoed Justice Chandrachud in rejecting originalist interpretation of the Constitution in light of the rapid changes in digital media which posed grave challenges to privacy.[183] He stressed that privacy has three aspects i.e. privacy of body (to move freely), informational privacy and privacy of choice (decisional autonomy).[184] The core values embedded in the Preamble, that of democracy, dignity and fraternity, he stated would be denuded without privacy

---

176 *Id.,* Part T (Our Conclusions) ¶3 (I).
177 *Id.,* Part T, ¶4.
178 *Supra* note 167, Justice Chelameshwar, ¶32.
179 *Id.,* ¶¶13, 14, 16, 17.
180 *Id.,* ¶¶43, 44, 45.
181 *Supra* note 167, Justice Bobde, ¶18.
182 *Id.,* ¶¶26-28.
183 *Supra* note 167, Justice Nariman, ¶¶64-66.
184 *Id.,* ¶81

and therefore, it was imperative to recognise it as a constitutionally guaranteed fundamental right.[185]

Further, Justice Sapre echoed Justice Chandrachud, Bobde and Nariman in rejecting originalist interpretation of the Constitution.[186] He also located the right as a core enunciation of the dignity of the individual as recognised in the Preamble.[187]

Justice Sanjay Kishen Kaul also supported Justice Chandrachud in differentiating between negative and positive obligations of the state in upholding the right to privacy.[188] Positive obligation requires legislative intervention by the state to protect *inter se* claims of violations of right to privacy.[189] What could be the possible harms which may result from privacy violations? This issue was eloquently addressed by Justice Kaul. Highlighting the idea of profiling as the automated processing of personal data to evaluate certain aspects about a natural person, Justice Kaul drew attention to the possibility of discrimination on the basis of caste, religion and ethnicity.[190] Intermediaries like Facebook, Google and Uber also collect large amounts of personal data and this can aid profiling which can then become the basis for influencing social behaviour and effecting representations which can muzzle dissent and thereby undermine democracy.[191]

Thus, harms are not only in the nature of private harms, but also can be characterised as constitutional harms. Cumulative impacts of privacy violations by both State and non-state entities like intermediaries' needs to be considered and for this we need to deepen the standard of review for such violations. This deepening can be effected in the following three steps. First, by differentiating between privacy infractions. Second, adopting a more stringent standard of review for relatively more serious privacy violations. Third, developing a referential standard (through the idea of constitutional morality) which frames privacy violations in terms of Constitutional harms. Each of these steps is discussed in detail in the following paragraphs.

Not all privacy claims are of similar value or should be granted the same level of constitutional protection. In this context, it is important to develop the distinction between privacy violations. Not all privacy violations result in imposing equal limitation on the individual.[192] Privacy violations can be categorised

[185] *Id.,* ¶85.

[186] *Supra* note 167, Justice Sapre, ¶15. This was also supported by Justice Sanjay Kishen Kaul, ¶33.

[187] *Supra* note 167, Justice Sanjay Kishen Kaul ¶¶8, 9.

[188] *Id.,* ¶12.

[189] *Id.*.

[190] *Id.,* ¶13.

[191] *Id.,* ¶19.

[192] Indeed Justice Chelameswar's concurring judgment refers to this distinction in the right to privacy case. Justice Chelameswar also suggested that not all privacy claims will attract constitutional protection and that there are species of privacy claims. Therefore, only those privacy claims which deserve the strictest scrutiny would have to pass the muster of twin tests of the law limiting

into two different species—privacy takings and privacy intrusions. These two species are primarily differentiated on the basis of the nature and extent of limitations that they impose on the individual. Privacy takings impose significant limitations on the individual and in effect render them substantially impoverished not only in terms of loss of autonomy over decision-making in the personal sphere, but also, complete and permanent extinguishment of this autonomy. In contrast, privacy intrusions refer to violations that are time bound in which there is a real possibility of restoration and therefore, restitution of autonomy over decision-making. Privacy intrusions should be legally tolerable upon explicit consent by the individual.

Privacy takings, both by the State and by non-state actors, should be prohibited as a general rule. The extreme deprivation that privacy takings entail makes the moral case for prohibition of privacy takings by private entities sufficiently clear. Even in cases of formal consent, therefore, the State should intervene to prevent such takings. Anita Allen in her book 'Unpopular Privacy' made a forceful argument supporting the role of the State in enforcing coercive privacy on "uneager beneficiaries".[193] There is a well established doctrine of non-waiver of fundamental rights which can be relied upon to support such a proposition.[194]

To establish whether a claim could be characterised as a privacy taking or a privacy intrusion it is also important to look at cumulative impact of practices rather than be confined to a specific instance related to the privacy claim. Apart from the moral argument, support for this line of legal argumentation can be based on the doctrine of non-waiver of fundamental rights. Privacy takings in exceptional circumstances may be permitted only by the State on the ground that it will attract the strict scrutiny standard of review.[195] The proportionality analysis in the strict scrutiny standard would include the necessity for undertaking such a measure and the State should have an additional burden of proving that it is least privacy restrictive.[196] The positive obligation of the State to uphold fundamental

---

the right to be just, fair and reasonable and that it fulfilled a compelling state interest (concomitant obligation for narrow tailoring).

193 Anita L. Allen, Unpopular Privacy: What Must We Hide? (2011)

194 *See* Basheshar Nath v. CIT, AIR 1959 SC 149. The Constitutional Bench of the Supreme Court of India held that "a large majority of the people are economic poor, educationally backward and politically not yet conscious of their rights. Individually or even collectively, they cannot be pitted against the State organizations and institutions, nor can they meet them on equal terms. In such circumstances it is the duty of the Court to protect their rights against themselves….fundamental rights created by the Constitution are transcendental in nature, conceived in national and public interest, and therefore cannot be waived". There was a 3:2 split in the Bench, with the former holding that all fundamental rights are non-waivable in character and the latter holding that only Article 14 deserves such standing.

195 This is as per allusion of Justice Chelameswar and Justice Sapre in their concurring judgment in the right to privacy case, providing for the "compelling state interest" test rather than the more lenient "legitimate state interest" test for reviewing privacy claims against the State. (*See* ¶124 of the Aadhaar judgment).

196 In the Aadhaar judgment, the Court interpreted the majority opinion of the Constitutional Bench (in the right to privacy judgment) as laying down the test of "legitimate state interest" rather than the "compelling state interest test" (the former being a more lenient test as it allows for a lower

right to privacy *inter se* also obligates it to ensure the application of the safeguard principle of ensuring no harm results from privacy intrusions.[197] This should also be viewed as a legitimate interest of the State. It is also important for the Court to appreciate that cumulatively singular privacy intrusions may result in privacy takings and therefore actively safeguard and review such privacy intrusions.

As was explicitly acknowledged by the constitutional bench of the Supreme Court in its judgment affirming the Right to Privacy, privacy as a normative value is intrinsic to the ideals of freedom, liberty and dignity of the individual as is recognised both in the Preamble and in the charter of fundamental rights in Part III of the Constitution of India.[198] It is therefore, a necessary condition for the functioning of the fundamental constitutional values and arguably stands at a higher pedestal than other derivative (and un-enumerated) constitutional rights (for instance the right to social entitlements as has been interpreted by the Court under Article 21). Indeed, Justice Bobde emphatically argued that privacy is the "basic, irreducible condition necessary for the exercise of personal liberty and freedoms guaranteed by the Constitution" and referred to it as the "inarticulate major premise in Part III of the Constitution".[199]

F. PRIVACY IN THE CONTEXT OF CONSTITTUTIONAL MORALITY

Given its constitutional primacy, this would entail the right to privacy being given the status of non-derogable and non-alienable fundamental right. This would imply that under no circumstances can this right be taken away by the State or other non-state actors even in case of extreme circumstances like a national emergency. Further, certain core aspect of right to privacy cannot be shared

---

burden of proof on the State in justifying any measure as in legitimate state interest as a permissible restriction on a privacy claim). The Supreme Court in the Aadhaar judgment applied the "legitimate state interest test" in undertaking the proportionality analysis looked at four aspects – necessity of measure (is it a legitimate state interest?); suitability of the measure in terms of the objective, existence of less restrictive but equally effective alternative and measure should not have disproportionate impact on right holder. I would argue that presuming the status of the right to privacy as non-derogable and non-alienable, demands that the condition of alternative measure be equally effective, be dropped. Thus it should be the exclusive burden of the State to establish the measure chosen is least privacy restrictive. Therefore, for all privacy claims which amount to privacy takings the Court should employ a "strict scrutiny test" that would require the State to establish the measure is in the nature of "compelling state interest".

197 The current statutory framework under the Information Technology Act, 2000 and the proposed Data Protection Bill only allows for due diligence obligations on intermediaries and the State in the collection and usage of personal data. However, the explicit recognition of a Constitutional Right to Privacy and the Court's earlier jurisprudence in the District Registrar and Collector v. Canara Bank, (2005) 1 SCC 496, case also entails the substantive extension of intermediary/State obligation to ensure that "no harm" results to the individual from the collection and deployment of personal data.

198 The majority judgement in the Right to Privacy case was discussed in the Aadhaar judgment. K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1 : 2018 SCC OnLine SC 1642, ¶81.

199 *Supra* note 167, Justice Bobde, ¶25.

even if the individual so wished. This is akin to the way the fundamental right to life and personal liberty under Article 21 of the Constitution is conceptualized as disallowing the right to commit suicide. The doctrine of non-waiver of fundamental rights is an established constitutional norm that would support such a conceptualization.[200]

If privacy takings are of the nature that cause not only extreme individual deprivation but also cumulatively lead to constitutional harms, it is imperative to enlarge the referential canvas to better appreciate their constitutional impact. Constitutional morality as a conceptual idea may provide us with more enriched canvas to review current developments.

Simply put, the idea of Constitutional morality refers to certain fundamental values embedded in the Constitution which requires protection *vis-à-vis* State action and inaction.[201] Further, Constitutional morality also requires that every public official as well private citizens would uphold these constitutional values through their actions. What are these fundamental values? These values are both which are expressly enumerated, for instance, the fundamental right guaranteeing life and personal liberty or democracy (provided in the Preamble to the Constitution) and unremunerated but which can be interpreted from the Constitution, such as federalism which has been identified as part of the *basic structure doctrine.*

Securing the dignity of the individual is one of fundamental values expressly enumerated in the Preamble to the Constitution of India. The Preamble to the Constitution was drafted as the Objectives Resolution ('OR') by Jawaharlal Nehru and passed on January 22, 1947 by the Constituent Assembly. The individual is given a primary position in the Preamble, since all powers and authority

---

[200] Basheshar Nath v. CIT, AIR 1959 SC 149, Constitutional Bench Decision of the Supreme Court which held that fundamental rights although individually exercised, is of such value to the constitutional fabric of India, that it cannot be waived off by individuals. This was a unanimous judgment on the point that Article 14 (Right to Equality) cannot be waived. The implication for the right to privacy would be that privacy interests cannot be waived off by the individual. This would mean that the state would have a role to play in intervening in contractual relationships inter se even where "consent" is provided amounting to waiver. Similar arguments have been made by Anita L. Allen, *supra* note 193, arguing for the role of the State in enforcing coercive privacy to uneager beneficiaries.

[201] The idea of Constitutional Morality was referenced only once in the Constituent Assembly by Ambedkar to argue that it is a virtue which is missing in India but needs to be cultivated. He meant it as allegiance to Constitutional values, i.e. both substantial values and structure of government. It has also been used by Supreme Court judges, specifically Justice Deepak Mishra, to refer to vaguely to certain actions as against constitutional morality (*e.g.*, State (NCT of Delhi) v. Union of India, (2018) 8 SCC 501).

It has also attracted some scholarly attention. *E.g.,* Pratap Bhanu Mehta, *What is Constitutional Morality?*, *We the People, A Symposium on the Constitution of India after 60 years, 1950-2010*, Seminar Magazine, November, 2010; Andre Beteille, *Constitutional Morality (Chapter 4)* in Democracy and Its Institutions (2012).

of the State is derived from the people.[202] Further, freedom of thought, expression, belief, faith, worship, vocation, association and action were expressly mentioned in the OR.

Similarly the idea of democracy was to embed a governmental system geared towards securing individual liberty of the people. The State was clearly subordinate to the people and only existed to realise the goal of individual liberty.[203] Dr. S. Radhakrishnan famously urged that it was necessary to safeguard the human spirit against the encroachment by the State. Therefore, although it was necessary for the State to regulate to improve economic conditions, this should never become so onerous so as to negate human spirit.[204]

Dr. B.R. Ambedkar preferred a parliamentary system of government over a presidential system, precisely because the latter better represented the idea of a limited and accountable executive since the executive was assessed daily by the legislative, which was a legitimate democratically representative of the people of India.[205] While supporting the adoption of panchayati raj, H.V. Kamath emphatically argued that we need to "try to make the State exist for the individual rather than the individual for the State."[206]

The dignity of the individual is protected not only by way of express enumeration in the Preamble but also by a series of choices in the structure of the government by way of democracy, by choosing *panchayati raj* institutions and choosing parliamentary form of government, all choices aimed towards securing the primacy of the individual and a limited government. The precise historical context of the partition and still nebulous nature of the Indian union (comprising of princely states and British provinces) made these decisions quite extraordinary given that one would have expected a greater emphasis on a stronger State.

Given this emphasis on securing the dignity of the individual, constitutional morality would demand that all institutions of the State – Executive, Legislature and Judiciary – as well as the citizens – uphold the dignity of the individual. If one accepts this position, this would allow us to completely reframe the right to privacy debate and expand the canvas to look beyond episodic potential harms to the individual. More fundamentally, it brings forth a need to review State actions such as the choice of collection of biometric data for authentication of beneficiaries, the ever expanding range of mandatory public service obligations which now require the use of Aadhaar, and the use of Aadhaar also by private non-state

---

[202] Jawaharlal Nehru while introducing the Objectives Resolution referred to them as "fundamental propositions" or values that would guide the framing of the Constitution. Constituent Assembly Debates, 13 December 1946 *speech by* Pandit Jawaharlal Nehru.

[203] *See* Constituent Assembly Debates, December 17, 1946 *speech by* Mr. M.R. Masani while supporting the inclusion of the term "democracy" in the Objectives Resolution.

[204] *See* Constituent Assembly Debates, January 20, 1947 *speech by* Sir. S. Radhakrishnan.

[205] *See* Constituent Assembly Debates, November 4, 1948 s*peech by* Dr. B.R. Ambedkar.

[206] *See* Constituent Assembly Debates, November 5, 1948 *speech by* Mr. H.V. Kamath.

entities. Quite simply, the question to pose is this: does these actions of the state, individually or cumulatively enhance or compromise the dignity of the individual? Given the internet relationship typologies mapped in the second section of this paper, the obvious answer is that it does compromise the dignity of the individual, as it allows for granular profiling of individuals in the citizens and this collection of information by the State and private intermediaries allows both these entities to have a disproportionate impact or influence over the lives of the citizens, by creating enormous potential for abuse. Sometimes the argument eludes us because we are unable to frame the correct question.

The limitations of the present framing of this debate in terms of individual harms and rationalising privacy takings through formal consent by individuals was made starkly evident in the decision of the Supreme Court in the Aadhaar case wherein the right to privacy was first applied. This is discussed in the next section.

G. THE AADHAAR JUDGEMENT

The right to privacy received explicit recognition by the Supreme Court, as a fundamental right under the Constitution of India in *K.S. Puttaswamy* v. *Union of India*.[207] It is important to note the constitutional implications of this recognition. This was first applied to review a claim that the Aadhaar project was violative of newly recognised right to privacy.[208] The Court upheld the Aadhaar project subject to specific conditions including the establishment of an effective data protection regime.[209] Despite its numerous faults, the Aadhaar project was found to be fulfilling the test of proportionality.[210] Significantly, the Supreme Court struck down Section 57 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 which allowed private entities to use Aadhaar information for authentication of identity.[211] Therefore, Government's recent endeavour to bypass this declaration and reinstate private access to data of citizens through a proposed amendment to the Aadhaar Act, 2016 is a significant development worth following.

In its decision, the Court argued that the majority judgement in the Right to Privacy case, laid down the 'legitimate state interest' standard rather than a 'compelling state interest' standard (as was mentioned by Justice Chelameswar and Justice Sapre).[212] The Court found that the measure, namely Aadhaar,

---

[207] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

[208] *Id*.

[209] *Supra* note 18.

[210] K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1 : 2018 SCC OnLine SC 1642 (Aadhaar judgment). References are made to the judgment as provided on the website of the Supreme Court of India in K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1 : 2018 SCC OnLine SC 1642.

[211] *Id.,* ¶219(e).

[212] *Id.,* ¶124. Majority judgment delivered by Justice Sikri on behalf of Chief Justice (Justice Deepak Mishra), himself and Justice A.M. Khanwilkar. It is interesting to note that even in Gobind v. State

passed the legitimate State interest test because the measure was proportional. Interestingly at the necessity stage, the Court found that the lack of an alternative measure, that would be equally effective but with a lesser degree of restrictiveness.[213] This begs the question that on whom should the burden rest of justifying the search of alternative measures and in defending the lack of alternative? Clearly it is the State who is proposing the measure. What is confounding is that the Court faulted the petitioner's failure to suggest alternative measures.[214]

On the question of balancing of two competing rights, the Court acknowledged that social entitlements are constitutionally protected and it ensures a right to live life with dignity.[215] The right to privacy also protects individual dignity. It finds that the measure is reasonable as it balances these two aspects of dignity since information collected at the time of authentication is minimal. This is a specious and circular argument. The challenge is not against the provisioning of social welfare benefits. The mechanism of delivering those benefits i.e. Aadhaar is privacy intrusive to say the least. Moreover, the Court is completely aware of its framing this as a facile trade-off since it states that "we are by no means, accepting that when dignity in the form of economic welfare is given, the State is entitled to rob the person of liberty. That can never be allowed. We are concerned with the balancing of the two facets of dignity."[216] This requirement of balancing would not have arisen in the first place if the measure in question was not Aadhaar, which requires the sacrifice of privacy by citizens in order to access their constitutionally protected social entitlements. In effect, by coercing citizens to make this choice between binaries, it fundamentally reduces social entitlements to privileges and citizens themselves to subjecthood.[217]

Here it would be appropriate to also discuss Justice Chandrachud's dissent on the application of the proportionality principle. He found that the cases cited to justify Aadhaar were inapplicable since those cases related to national security and prevention of crime.[218] He held that the collection of demographic and biometric information in the Aadhaar project, effectively justified the treatment of all citizens as criminals without making a distinction for those indulging in identity fraud and therefore infringed upon the justifiable expectations of privacy of ordinary citizens.[219] Thus he held Aadhaar to be disproportionate to the objective sought to be achieved by the State.

---

of M.P., (1975) 2 SCC 148, the test suggested was the compelling state interest standard rather than legitimate state interest standard, to review privacy claims.

213 *Id.,* ¶280.

214 *Id.*

215 *Id.*, ¶¶447, 2(h)(ii).

216 *Id.*, ¶¶447, 2(j).

217 Bidisha Chaudhuri & Lion König, *The Aadhaar Scheme: A Cornerstone Of A New Citizenship Regime In India?*, 26(2) Contemporary South Asia 127-142 (2018).

218 *Supra* note 210, ¶217. (Justice Chandrachud's dissent in the Aadhaar judgment)

219 *Id.*

The Aadhaar judgement of the Court reflects its failure to appreciate the current reality of how information is collected, stored and shared and also the inability of individuals to assess and negotiate singular actions of information sharing and differentiating them from the cascading effects of information merging and the potential harms which may result from the abuse of such data convergence.[220] This failure is also more problematically reflected in the continued emphasis on individual consent as the fundamental principle for allowing for privacy intrusions, when in fact individuals have little knowledge, information or agency in negotiating such acts of sharing of privacy. This is also reflected in the Court's acceptance of the "voluntariness" of Aadhaar as per Section 3 of the Aadhaar Act, even though such voluntariness is coercively obtained by making it mandatory for accessing social entitlements under Section 7 of the Aadhaar Act, 2016.[221]

IV. INDIA'S CURRENT LEGISLATIVE AND POLICY FRAMEWORK ON PRIVACY

The Indian legislative framework on privacy specifically in the context of the digital space is provided for in the Information Technology Act, 2000 and the Indian Telegraph Act, 1885. The Telegraph Act has been used by the government to stipulate license conditions including stipulations on security of data being transmitted through the network accompanied by some exemptions for public security.

Under the IT Act, Section 66E stipulates that

> "Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both."

The two key definitions are that of "private area" and "under circumstances violating the privacy". The definition of private area is limited to genitals, pubic area, buttocks or female breast. Further, the latter definition also focuses on the reasonable expectation of privacy in spaces where private parts of the body may be exposed.

---

[220] For instance, as Justice Chandrachud underlines in his dissent, the metadata can also be collected through noting of IP address of the location from which authentication requests are made.

[221] Justice A.P. Shah, *Why the Supreme Court's judgement on Aadhaar is flawed*, Scroll, Jan 22, 2019, available at https://scroll.in/article/909959/supreme-courts-aadhaar-judgement-created-a-gaping-chasm-in-society-writes-justice-ap-shah (Last visited on February 20, 2019).

This exclusive focus on body parts as private reflects an earlier construction of privacy violations which we find in the Indian Penal Code ('IPC'). Under the IPC, Section 509 (outraging the modesty of women) and Section 354C (Voyeurism) focuses on women related offences. Section 72 under the IT Act provides for penalty for breach of confidentiality and privacy. The breach is triggered by non-consensual disclosure of electronic information, correspondence. This presumes that personal data is private and therefore, cannot be disclosed without consent. However, given that there is no definition of "personal data" within the Act, it means that data protection is very much regulated through contractual definitions.[222] However, there is a *non obstante* clause provided under Section 79 of the IT Act, which only makes the intermediaries liable in the event of failure to take due diligence obligation. This in itself provides for insufficient sanction or for that matter adequate incentive to actively develop systems for securing data privacy.

Overall one can identify three serious drawbacks of the current legislative framework. First, the idea of what should be private and therefore protected is extremely limited to either parts of the physical body and health or financial information. This leaves out a vast amount of data which is generated through private activities both on the internet and on telephony and exposes the user to a range of moral violations including snooping of personal activity, profiling and data thefts. In this context, it is pertinent to note that the "reasonable expectation of privacy" standard as elucidated by the Court in the Aadhaar case[223] includes the consideration of aspects such as whether the information is previously disclosed publicly is problematic. Disclosure of personal information even publicly may be accompanied with the expectation that such information will not be abused or used to discriminate and socially disadvantage. This is evident from the ratio in the Phoolan Devi case. Further, the idea of serious or significant injury should be limited to not only private harm but also constitutional harms as discussed in the previous section.

Second, the due diligence obligation is clearly inadequate and allows intermediaries to escape liability even in case of data breaches. A due diligence standard is therefore unhelpful in both incentivizing adoption of better data security measures internally or enough of a sanction to penalise repeat offenders from allowing for data breaches. Third, data privacy cannot be protected through a regime of contractual consent. Consent as we all know operates in the ideal scenario where negotiating parties are similarly situated in terms of resources and knowledge. This is not the case between intermediaries and users which is characterized by immense knowledge asymmetries, differences in technical capacities and negotiating capacity. The current law as it stands is therefore, completely inadequate to ensure substantive consent while securing data privacy. It is also for this

[222] There is however, a definition of "sensitive personal data" which relates to health and financial information under the Information Technology (Reasonable Security Practices And Procedures And Sensitive Personal Data Or Information) Rules, 2011 issued under the IT Act.

[223] *Supra* note 210, ¶292.

reason, Ministry of Electronics and Information Technology (MeitY) has recently been mandated to develop a Framework for Data Protection Law for protection of online personal data. The constitutional bench of the Supreme Court in the K.S. Puttaswamy *case* (Right to Privacy judgement) has also suggested that the government should legislate a data privacy law to ensure that the fundamental right to privacy is adequately protected also in the case of *inter se* relationships between private legal entities.

V. CONCLUSION

The right to privacy is an emanation of the right to self determination of an individual. The role of the State in delaying the provisioning of a robust data protection framework for ensuring this right in the digital space should be suspect, especially given that it is an "interested party" in increasingly using internet and specifically private intermediaries for a range of public functions.

The Right to Privacy judgement located the philosophical basis of the right to privacy as inalienable natural right that seeks to protect the dignity and autonomy of the individual. This is one of the fundamental values on which India as a constitutional republic was founded. Privacy takings and privacy intrusions both significantly undermine the autonomy of the individual and the right to self determination. In the internet era, privacy takings and intrusions are manifestly more insidious and multiple. It is imperative therefore to develop an understanding of these infractions and to examine them in light of constitutional morality. Perhaps the idea of not only personal harm but also potential constitutional harm to the republic should be developed to better appreciate the cumulative implications of these developments.

In the final analysis we need to look at the internet as allowing for a collective range of relationships that mutually reinforce each other. In such a context, a pursuance of narrow legalistic analysis of constitutional provisions and assessment of actions which may potentially violate such provisions are of limited utility. Constitutional theory and jurisprudence is also a rich source of fundamental political values which I refer to as constitutional morality. Contemporary developments like the rapid intrusion of the internet into the public and the private life of the Indian citizen can undermine constitutional morality in terms of fundamentally altering the relationships between the citizen and the state and between citizens inter se. It may lead to a greatly unequal public sphere and fundamentally compromise the individual right to self determination and autonomy of choice which privacy seeks to protect and nurture.

The idea of constitutional morality refers to the fundamental values that are explicitly mentioned in the preamble to the Constitution. It is also necessary to examine the Constituent Assembly debates to provide us an insight into the context in which such fundamental values were sought to be protected through

the guarantee of fundamental rights and the administrative structures that govern the institutional functioning of the constitutional authorities which were tasked with the safeguarding of those values.[224] An imagination of constitutional morality should permeate the actions of all constitutional functionaries including the executive.[225] This will also allow for self evaluation by the executive in undertaking legislative measures such as Aadhaar which are essentially in the nature of a privacy taking or to aggressively intervene in safeguarding privacy takings and intrusions by non-state actors.

The idea of constitutional morality provides us the imaginative and the legal space to examine current practices on the internet in reclaiming the debate in terms of the fundamental values. Our inability or unwillingness to respond to the challenges posed by the rapid penetration of the internet and that of big data would reduce citizens to nothing more than the crocodiles in Alipore Zoo, whose privacy is a privilege granted only when it is deemed to be productive by others (be it the executive or by commercial enterprises in search of good quality 'data' to design models for artificial intelligence).[226]

---

[224] For instance, the Constituent Assembly debated the idea of parliamentary versus a presidential system of government based on the tradeoff between stability and the responsibility. The choice of a parliamentary system reflected the importance of executive responsibility to the legislature. The passage of the Aadhaar Act as a money bill denied full legislative scrutiny to an executive act and in effect gravely undermined the fundamental reasons why our constitutional framers had chosen the parliamentary system in the first place. Thus reflection from the context of constitutional morality is more substantive and enriching that an impoverished analysis of applicable legal provisions which would state that the decision of the speaker is final in terms of notifying a bill as a money bill and therefore the determination by the speaker will pass constitutional muster.

[225] Justice Chandrachud underlines this point when he wrote that "a ruling government has to work within constitutional parameters and has to abide by constitutional morality"; *supra* note 210, ¶100 (Dissenting judgment in the Aadhaar case).

[226] *See, e.g.*, Imanol Arrieta Ibarra et al.; *Should we treat Data as Labor? Moving Beyond "Free"*, 1(1) American Economic Association Papers & Proceedings (2018). (Arguing for the adoption of "data as labor" paradigm wherein individuals should become self conscious sources of good quality data and be remunerated for it so as to aid in the creation of robust Artificial Intelligence which is expected to automate half of the jobs in the market to the disadvantage of those very individuals.)