Honorary Advisors

1. **Remembering Hon’ble Justice (Dr) A. S. Anand**, 29th Chief Justice of India, Former Chairman, NHRC
2. **Hon’ble Justice Arjan Kumar Sikri**, Former Judge, Supreme Court of India
3. **Hon’ble Justice K. S. Panicker Radhakrishnan**, Former Judge, Supreme Court of India
4. **Hon’ble Justice Prakash Prabakar Naolekar**, Former Judge, Supreme Court of India, Former Lokayukta, Madhya Pradesh
5. **Hon’ble Justice Peter Mohan Peiris**, 43rd Chief Justice of the Republic of Sri Lanka
7. **Prof. (Dr.) Ranbir Singh**, Vice-Chancellor, NLU, Delhi
8. **Prof. (Dr.) Mahendral Pal Singh**, Chancellor, Central University of Haryana
9. **Prof. (Dr.) Faizan Mustafa**, Vice-Chancellor, NALSAR Hyderabad
10. **Prof. (Dr.) R. Venkata Rao**, Vice-Chancellor, NLSIU Bengaluru
11. **Prof. (Dr.) Shashikala Gurpur**, Director, Symbiosis Law School, Pune
12. **Prof. (Dr.) A. Lakshminath**, Former Vice-Chancellor, CNLU Patna
13. **Prof. (Dr.) Sukh Pal Singh**, Former Vice-Chancellor, HNLU Raipur
14. **Prof. (Dr.) Paramjit Jaswal**, Vice-Chancellor, RGNUL Patiala
15. **Prof. (Dr.) Rose Varghese**, Former Vice-Chancellor, NUALS Kochi
16. **Mr. Arvind Datar**, Senior Advocate, Supreme Court of India
17. **Mrs. Geeta Luthra**, Senior Advocate, Supreme Court of India
18. **Dr. Adish C Aggarwala**, Sr. Advocate & President of International Council of Jurists
19. **Ms. Maneka Guruswamy**, Senior Advocate, Supreme Court of India
20. **Ms. Karuna Nundy**, Advocate, Supreme Court of India
21. **Prof. S. Sivakumar**, Member, 21st Law Commission of India (2016-18)
22. **Prof. Michael Keating**, Director, Center for Constitutional Change, University of Aberdeen
23. **Prof. Richard Albert**, Professor, University of Texas
24. **Prof. Andrew James Harding**, Professor of Law, National University of Singapore
25. **Prof. Madabhushi Sridharacharyulu**, Former Central Information Commissioner
Esteemed Members

1. **Dr. Satish Gowda**, Senior Professor of Law, P.G. Department of Law, Bangalore University, Bengaluru, Honorary Member, Advisory Council
2. **Dr. Atmaram Shelke**, Assistant Professor, Symbiosis Law School, Pune
3. **Mr. Mohd Imran**, Asst Prof., School of Law & Constitutional Studies, Shobit University, Meerut
4. **Adv. Manjeet Kumar Sahu**, Advocate, High Court of Jharkhand
5. **Ms. Navtika Singh**, Assistant Professor, ICFAI University, Dehradun
6. **Adv. S. Basavaraj**, Advocate, Karnataka High Court, Daksha Legal Advocates, Bengaluru, Honorary Member, Advisory Council
7. **Ms. Sanya Yadav**, Assistant Professor, Amity Law School, Jaipur
8. **Mr. Niteesh Kumar Upadhyay**, Asst. Professor, School of Law, Galgotia University, Founder, Knowledge Steez

*Founding Board (Permanent Members)*

Sameer Avasarala, Founder Editor  
Shashank Kanoongo, Founding Editor  
Samiya Zehra, Founding Editor

*Core Team*

Ankita Aseri, Publishing Editor  
Anubhuti Maithani, Deputy Publishing Editor  
Amit Singhal, Editor-in-Chief  
Aswinikumar Bairagya, Deputy EiC  
Kriti Johri, Senior Editor

*Sr. Associate Editors*

Mahvish Shahab  
Promita Sinha

*Associate Editors*

Shreetama Ghosh  
Mythili Mishra  
Aanchal Pandey  
Aparajitha Jha  
Nipuna Varman  
Velpula Auditya  
Ankit Tripathi  
Anisha Singh  
Lakshmi Menon  
Shipra Sayal  
Aditi Duggal  
Mohit Vats  
Anushka Sharma  
Naina Nerli  
Sonal Gupta  
Tanya Arora
## Contents

**PRESIDENTIAL PARDONING POWER, JUDICIAL REVIEW, AND THE NEW FACE OF ‘MERCY’: AN EXAMINATION OF THE EXERCISE OF PARDONING POWER IN NIGERIA AGAINST THE CONSTITUTIONAL DEVELOPMENT IN INDIA** .............................................. 8

**CONSTITUTIONAL & LEGISLATIVE FRAMEWORK OF THE CIVIL SERVICES IN INDIA IN CONTEMPORARY WORLD SCENARIO** ............................................................... 37

**NRC IN ASSAM: ANALYSING THE QUESTION OF CONSTITUTIONAL MORALITY AND LEGAL RATIONALITY** ........................................................................................................ 61

**FAKE NEWS: A CLEAR LOOK BEYOND THE VAGUENESS** .......................................................................................................................... 72

**THE ESSENTIAL RELIGIOUS PRACTICES DOCTRINE: ITS FALLACY AND FUTURE** .......................................................................................................................... 86

**CONVENTION ON THE RIGHTS OF PERSONS WITH DISABILITIES & DILUTION OF SEPARATION OF POWER BY THE SUPREME COURT: A BENEVOLENT HYPOCRISY** .......................................................................................... 92

**ANALYSING THE PRACTICAL IMPLICATIONS OF A RIGHT TO PRIVACY: STATE SURVEILLANCE AND CONSTITUTION** .......................................................................................... 99

**ENFORCEMENT OF UNCONSTITUTIONAL STATUTES** .......................................................................................................................... 119

**BALANCING CONSTITUTIONAL MORALITY AND RELIGIOUS FAITH: THE DISPUTE OVER RIGHTS AROUND SABARIMALA ISSUE** .......................................................... 136

**VIRTUAL CENSORSHIP IN THE ERA OF ONLINE STREAMING: THE CHALLENGES AND CONSEQUENCES** .......................................................................................................................... 150
ANALYSING THE PRACTICAL IMPLICATIONS OF A RIGHT TO PRIVACY: STATE SURVEILLANCE AND CONSTITUTION

Authored by Anubhav Khamroi & Anujay Shrivastava*

ABSTRACT

Privacy is the most revered right in our society, integral to human existence, however, always the greatest bugaboo for the State. State Courts, across jurisdictions, have been extremely impetuous in adopting privacy as their go-to justification, without adequately clarifying the import and scope of “privacy” as a right. Such “incoherence” in judicial decision-making significantly impacts doctrinal clarity and conceptual consistency. Furthermore, the varying theories on privacy have also contributed to its theoretical indeterminacy. In this Paper, we shall evaluate and critique the existing ideas and notions of privacy, while also attempting to draw out an alternate theoretical framework, in order to address the demands of contemporary digital world. We believe at a time when there is increasing surveillance by both State and Non-state actors, it is imperative to rethink the contours of “Privacy”. Further, we have addressed the contemporary privacy concerns by evaluating the risks of potential breach by social-media forums, such as Facebook and Google, and argued that “threat on privacy” is not necessarily akin to “loss or breach of privacy”. We have also attempted to deal with the issue of right to privacy over “documented personal information”, in light of the recent Aadhaar judgement. On that note, we have inquired into the proportionality test adopted by the Indian Supreme Court in the landmark Puttaswamy decision, and then compared it with similar tests used in foreign jurisdictions to adjudicate the legality of State surveillance programmes.

Key Words: Aadhaar, Control, External Interference, Informational Privacy, Internal Reservation, Limitation, Personal Information, Privacy, Social-Media.

INTRODUCTION

“Privacy” is one of the most cherished right in human society. Yet, unfortunately, privacy has historically been a nebulous concept, constantly evading the ‘trap’ of a singular definition.
However, philosophers and legal scholars have also been equally adamant and have constantly made efforts to create a linear narrative of “Privacy”. Today, while there exists a structured discourse on privacy, in both philosophical and legal terms, we are yet to formulate a practical definition of privacy which can meet the demands of the fast-evolving digital world.

Unfortunately, in recent times, the judicial trend has predominantly been to apply “privacy” to a wide range of cases, without sufficiently clarifying the scope and contours of such a right. This regrettably adds an ad-hoc flavour to adjudication and departs from the longstanding principle of “coherence” in judicial decision making.242 The final decision or outcome of a case is important indeed, but the means or reasons underlying that final outcome are equally significant.

Recalling the words of Prof. Pritam Baruah (in an article discussing core principles of adjudication) –

“Answers to the theoretical questions are the basis for decisions on specific issues before a court. Answering the theoretical question demands an explanation of the concepts that a court employ. This must be an explanation in terms of reasons, which explain why courts take a particular view of the concepts involved and not another. Courts need to establish a connection between what they take the concepts to be, the specific rights that are being debated, and what is required by the application of those concepts. Here one might object that courts often do not fully explain the reasons for a decision…” [emphasis added].243

Sharan, Judicial Clerk to Hon’ble Mr. Justice L. Nageswara Rao, Supreme Court of India, for their feedback and guidance. An earlier version of this Article was presented in a seminar by Mr. Khamroi for the Elective Course titled “Constitutional Values in Courts: Dignity and Liberty” taught by Prof. Baruah from February to May 2018, at O.P. Jindal Global University, Sonipat. This Article is a follow-up to an earlier Article published by the authors in: Anubhav Khamroi & Anujay Shrivastava, The curious case of Right to Privacy in India, 2(12) Indian Constitutional Law Review 1-2 (2017), and focuses on “Informational” aspect of Privacy. Mr. Shrivastava had subsequently published a follow-up Article to the preceding Article on “Decisional” aspect of Privacy in: Anujay Shrivastava, Reconstructing the Decisional Paradigm of Privacy: Crafting a new Anti-Manifesto Grounded on Shadows of The Enabling School, 6 Indian Constitutional Law Review 7-23 (2018). The authors recommend these Articles for a further read on Privacy. However, responsibility for the ideas expressed or/and any mistakes in the present Article are entirely theirs. Authors can be reached at 15jgls-akhamroi@jgu.edu.in and 15jgls-ashrivastava@jgu.edu.in.

---

In our opinion, such decisions play a lead role in creating an undesired haziness in the discourse and jurisprudence on privacy. Further, this “situation of conceptual bankruptcy”, wherein we understand privacy as a “bundle of rights” leads to juxtaposition of the specific roles of one onto the other.

In this paper, we shall set out to evaluate and analyse the existing formulations of “Privacy” and subsequently propose an alternate structure to the discourse on Privacy, suitable to the contemporary needs. Therefore, in Part I, we shall analyse and critique the existing theories of Privacy, primarily - Thomson’s and traditional notions of privacy, Control-based theory, Accessibility-based theory, and W. A. Parent’s “New Definition”.

Further, in Part II, we shall attempt to draw out a conceptual framework by providing an alternative definition of Privacy, in light of contemporary technological advancements. Our definition shall try to address the drawbacks of the existing theories, and will apply to both “documented” and “undocumented” personal information. According to W.A. Parent, “documented personal information” includes publicly available information, such as police records, court proceedings and judgements, government archives, public inspection reports etc. According to him, “documented personal information” is not protected by Privacy and argues that its inclusion within the Privacy framework would “needlessly blur the fundamental distinction between the private and the public.” We shall put forth our disagreements with such a restrictive understanding of Privacy in the latter sections of our Paper.

In Part III, we attempt to take the proposed definition forward and inquire into the scope and effects of such a right in protecting “undocumented personal information” available on social media sites or stored in an electronic database. We shall rely on the ideas of “legitimate expectation of privacy” and “threatened loss counterexample” to address the risks of potential breach vis-à-vis the right to privacy. We shall conclude this section by arguing that mere “threat on privacy” is not necessarily akin to “loss or breach of privacy”. In Part IV, the Paper shall address the operation of right to privacy over “documented personal information”, in the context of the recent Aadhar judgement

---


245 Id.

246 Id.

247 Id., at p. 347.
In **Part V**, we shall analyse the scope of limitations on Privacy in Indian constitutional jurisprudence and consequently, consider situations wherein State surveillance ‘may’ pass constitutional muster. Finally, in **Part VI**, we shall attempt a comparative analysis (or a *tour d’ horizon* study) of several foreign decisions, which had considered the legality and constitutionality of State surveillance programmes. This is to understand how different courts have articulated the confines or limits of right to privacy and tests adopted to evaluate the legality of legislative actions.

**Part I. ADDRESSING THE SITUATION OF “CONCEPTUAL BANKRUPTCY”: CRITIQUE OF THE EXISTING THEORIES ON PRIVACY**

Privacy must be understood as a right which prevents unwanted access to “personal information” and impede any non-consensual/wrongful attempts at acquiring such information [explained in **Part II**]. However, there are several theories on Privacy which confuses its application with that of other concepts like Liberty, Autonomy, Dignity, Solitude, and has therefore transformed Privacy into an indeterminate concept. It shall be our endeavour to evaluate the major theories on Privacy and point out the flaws in them.

**(a) Privacy as a “bundle of rights”: Traditional Understanding**

At the outset, we strongly disagree with the idea, advocated by Thomson and other ‘traditional’ privacy theorists, that privacy has no single meaning. According to this traditional account, privacy stems from a diverse set of rights, such as “right to freedom from disclosure of personal information”, “independence in making fundamental decisions without coercion”, “right to make bodily decisions”, etc.248 All cases involving the aforementioned questions of law can be resolved by an appeal to various other constitutional values, such as “Liberty and Self-Determination”, “Autonomy or Freedom of Choice”, “Right against trespass”, “Tort of Nuisance” etc.

Posner rightly opined - “*we already have perfectly good words - liberty, autonomy, freedom to describe the interest in being allowed to do what one wants (or chooses) without interference. We should not define privacy to mean the same thing and thereby obscure its* .......
Thus, there is no need to unnecessarily expand and obscure the meaning of Privacy.

In our opinion, legal scholars and courts across the world are equally responsible for creating the unnecessary haziness in the discourse on Privacy. Over the years, courts have used Privacy to justify their judgements in several cases, where they could have simply used other, and much more contextually appropriate, constitutional values and principles. We would like to put forth three decisions of the US Supreme Court as appropriate illustrations of our claim:

**Illustration I:** In *Griswold v. Connecticut* (1965), the US Supreme Court was hearing a challenge to a law forbidding the use of contraceptives. The Supreme Court struck it down on the ground of violation of right to privacy. However, in our opinion, the Supreme Court could have easily used more suitable constitutional values such as Liberty, Autonomy or even Right to Life.

**Illustration II:** In *Loving v. Virginia* (1967), the US Supreme Court was adjudicating a challenge to a statute that prohibited certain marriages solely on the basis of racial classification. The Supreme Court struck down the statute and subsequent decisions have read this decision as establishing “a right to privacy in marriage-related choices”. However, in our opinion, the Courts would do better to use other principles such as Right against discrimination and Personal Liberty.

**Illustration III:** In *Stanley v. Georgia* (1969), the US Supreme Court was deciding the challenge to a Georgia statute that made mere private possession of obscene material an offence. The Supreme Court struck down the statute on the basis of a right to privacy vis-à-vis right to control one’s thoughts violation. Alternatively, the Supreme Court could have *simply used* Freedom of Speech and Expression, Liberty, Autonomy as grounds to strike down the law.

(b) **Control-based theory of privacy**

Control-based theories of Privacy state that one should have absolute control over one’s personal information and be able to share it at its own will. “Control” would include the “ability to prevent disclosure of personal information to individuals, other than those to

---

whom we have voluntarily revealed it”. 254 However, the ability to exercise “control”, which is synonymous to the absence of coercion, is not always a necessary pre-condition to the enjoyment of Privacy.

For example, in cases of disabled persons, comatose patients and patients suffering from acute paralysis, the privacy of those individuals is protected at all times, through their family members and doctors [sharing a “privileged relationship”], even though those individuals lack the ability to exercise “effective control” over their own acts. In this context, Vincent J. Samar255 presents an illustrative contrary example by noting that – while prisoners have the absolute ability to exercise “control”, they may not be free from the gaze of the guards and thus, does not effectively enjoy Privacy.

(e) Accessibility-based theory of privacy

Accessibility-based theories conceptualize Privacy as one’s right to take away the ability of others to access or acquire their personal information. 256 According to such theorists, the mere possibility that others could acquire personal information constitutes a violation, even when there is no actual attempt to acquire it. 257 Such an account of privacy would render all forms of surveillance, state welfare & census programs, a doctor-patient, a lawyer-client relationship illegal and purposeless.

(d) W.A. Parent’s “new definition” of privacy

W. A. Parent defines Privacy as “not having undocumented personal information about himself known by others”. 258 We strongly disagree with his idea of acquisition of “undocumented personal information” as the only ground for invoking right to privacy. Parent’s own account could lead to undesirable results when tested against the counterexamples he himself used to attack other theories. If we follow his definition, then an attempt to acquire personal information, which is already available in public records, by an unknown person/entity from private spaces of an individual by using X-ray devices would

254 Id.
not constitute a violation of Privacy.\textsuperscript{259} Thus, the definition partly fails due to this erroneous classification.

\textbf{Part II. RETHINKING THE CONTOURS OF “PRIVACY”}

We endeavour to provide an alternate structure to the discourse on privacy. Accordingly, Vincent had opined -

\begin{quote}
\textit{“a \textit{judicially useful} definition of privacy must take into account \textit{the effect} that one's actions may have on society, so that the concept \textit{is not broader than the ultimate value} under which action will be allowed” [emphasis added].}\textsuperscript{260}
\end{quote}

We believe a useful and substantive definition of Privacy shall possess the ability to answer the following two questions:

1. Why do we need Privacy as a separate and distinct right?
2. What would be the exact scope and limits of such a right?

\textbf{(a) Why do we need privacy as a separate and distinct right?}

We shall commence by outlining the purpose of having a separate right to Privacy (subject to the specificities of the jurisdiction in question), which has been commonly referred to as an “empty vessel” or a “hypothetical right”.\textsuperscript{261} It is imperative to note that other constitutional values, such as liberty, autonomy, dignity provide agency to an individual to perform certain private acts, without any “external interference”. However, these values do not affect the psychological aspects of the acts committed by a person. Privacy plays an important role in allowing an individual to shape their “personality” in a manner they desire, which is a necessary pre-condition to the performance of a private act without any “\textit{internal reservation}”.

We propose to draw this distinction between “external interference” and “internal reservations”, in an attempt to better explain the import and scope of Privacy. While we generally tend to focus on “external interferences” in our private lives, we often fail to give much attention to the “internal reservations” we hold due to the fear of making our “personal information” publicly available. In this context, it is of utmost importance to explain the meaning of “internal reservations” with great care.

We use the term “internal reservation” in context of a person who has both the intention and the ability to partake in a private act but is dissuaded due to an unknown fear of divulging “personal information” integral or incidental to that act. Thus, it has a subconscious effect on our minds, which creates a disparity between “what we desire” and “what we actually end up doing”. It is imperative to understand that protecting any information integral or incidental to a private act is equally important for the successful performance and future continuance of such an act, and thus, ought to be protected at a level equal to the act itself.

“Internal reservations” come into the picture even before the person has performed the private act, and causes greater damage to the person’s personality, than interferences from third parties. We submit that - Privacy is the value that addresses the issue of “internal reservations”, by protecting all information integral and incidental to the private acts of a person, which are done in exercise of their liberty or autonomy. Furthermore, Privacy also precludes all means of collecting such private information.

(b) What would be the exact scope and limits of such a right?
In our opinion, the Right to Privacy can be defined as the “right to prevent others from wrongfully, non-consensually or illegally accessing and/or misappropriating personal information, notwithstanding the public availability of such information.” Here, it is imperative to subject every word of the above definition to careful scrutiny and thus, can be broken down into 3 parts:

i. **Wrongful, non-consensual or illegal**: right to impede others from accessing one’s personal information and consequently using it in a manner that was never consented to by the person, whose personal information is in question, or obtaining such information by violating the law or breaching an existing contract. The value of “consent” plays a significant role in our account of Privacy.

ii. **Personal information**: Information that one does not want to be out in public, due to various reasons, including the fear of being misrepresented to prospective employers, spouses, colleagues etc. It would also include information available in public records. Moreover, the nature of the information is of no consequence i.e. sensitive or mundane in cases of breach of privacy, as has also been held in several judicial.

---

iii. **Private:** It would include any private space, including “virtual spaces” of individuals on social media interfaces.

iv. **Access and/or misappropriate:** Both are independent violations and are neither inter-linked nor inter-dependent.

For Point (iv), it is necessary to clarify that, according to this definition, a privacy violation shall occur as soon as there is any “wrongful” access/acquisition of personal information, and there is no need to wait till the acquired information is misappropriated or a private act is hindered on the basis of such information. We would like to use a few examples to explain the operation of above definition:

**Example I [wrongfully/non-consensually accessing personal information]:** A and B want to partake in consensual sex and do so without informing anyone i.e. a third party. Their intimate act is protected from any external intrusion by values such as Liberty or Right to lead a meaningful Life or Autonomy. But any information integral or incidental to the act, such as place and time of the act; whether they used contraceptives; whether the act was hetro-sexual or homo-sexual in nature; is to be protected by Right to Privacy. Such personal information is integral to the act and if C [a third party] is attempting to collect such information by peeping through the window or by using an X-ray machine to look through the walls, then that would constitute a Privacy violation.

**Example II [misappropriation of consensually acquired personal information]:** A and B get involved in a consensual sexual relationship and after a few days B informs her/his sister. Now, even after acquiring such information, B’s sister cannot interfere as their private acts are protected under guarantees of Liberty or Autonomy. Moreover, she also cannot divulge such “personal information” to any third party without the consent of A and B [Not A OR B, consent of both the parties is required], as that would constitute “misappropriation of personal information”.

**Example III [notwithstanding the public availability]:** X is a famous Bollywood celebrity and his pictures are all over the internet, newspapers, magazines etc. However, if Y tries to use an X-ray Camera to look through the walls of his bedroom and click his pictures, that would constitute a major privacy violation. Therefore, the definition protected “personal information”, even if they are already available in the Public.
Part III. RIGHT TO PRIVACY VIS-À-VIS “UNDOCUMENTED PERSONAL INFORMATION”: CONTROL VS. PRIVACY DEBATE

In cases of social media sites/platforms, there exists a notion that we lose “control” over our personal information and the owners of those sites gain “access” to them, once the information has been shared with them using their interface. However, we shall argue that –

i. *First*, it is not necessary to provide any “personal information” to avail their services, other than very basic information like name, age, country etc., which is necessary to verify that one is a bonafide user;

ii. *Second*, once we have availed their services, it is our own decision to share any “personal information” using their interface, which in itself involves a genuine exercise of “control”; and

iii. *Third*, even if there is a subsequent “loss of control”, that does not necessarily entail a “loss of privacy” over personal information.

No matter what, every individual retains their right to privacy over personal information, even though that information exists only on a virtual space.264 There undoubtedly exists a right to prevent the owners of those sites from “wrongfully, non-consensually or illegally accessing and/or misappropriating” whatever information was shared using their interface or was stored in their database. An act of voluntarily sharing personal information over virtual public interfaces does not automatically extinguish the “Legitimate Expectation of Privacy” of the person disclosing such information.265 This is even more true in the contemporary age as people disclose tons of personal information to third parties, while doing the most monotonous activities.

It is certainly admitted and acknowledged that Facebook, WhatsApp, Gmail and all other social media platforms, have the “hypothetical ability” to access our personal information, which is being shared using their interface. However, the possibility of such a breach actually happening is extremely low, subject to certain exceptional cases. This is even more true in light of the recent **EU General Data Protection Regulations**266 [hereinafter, “GDPR”] and similar **Telecom Regulatory Authority of India** guidelines with regard to **Data Privacy, Data Protection and Cyber Security**.

---

These regulations strengthen the philosophy underlying our definition of Privacy, which helps in shaping one’s personality and enables the person to freely exercise liberty or autonomy without any “internal reservation”. Therefore, as per our definition, if the operators of Facebook/Google attempt to access the user’s private data, their acts would fall foul as being “non-consensually or illegally accessing personal information”. Funnily enough, “Calm” – a meditation and sleep assistant software, has recently added the full text of GDPR to its collection of sleep stories and apparently “a brief listen to it will be enough to cure even the most wide-eyed of insomniacs”.267

In any event, it is not to be forgotten that it is a result of our own “choice” to – firstly, use their interface and avail their services; secondly, voluntarily share personal information which we would not have otherwise shared in a public space; and thirdly, to do so with the knowledge of their “hypothetical ability” to cause a potential breach. Moreover, the standard of “hypothetical ability” is too vague to make a strong allegation of privacy violation against the owners of the social media sites.268

Moreover, their “hypothetical ability” to access and misappropriate one’s personal information does not necessarily mean that one no longer enjoys the right to privacy over that information.269 While the loss or lack of control undoubtedly “threatens” privacy and creates a risk of potential breach, it does not necessarily involve a “breach of privacy”. Thus, a mere “threat to privacy” is not necessarily akin to “loss or breach of privacy”.270

The above argument can be better explained by employing the idea of a “threatened loss counterexample”. One such illustration of a “threatened loss counterexample”, could be found in Parent’s work –

“Suppose A invents a fantastic X-ray device that enables him to look right through walls. A then focuses the device on my home but refuses to use it. Since he certainly has the power to find out everything that I am doing in my home it cannot be said that I any longer enjoy control over personal information about myself vis-a-vis A…. Still

A has not invaded my privacy. He doesn't do that until he actually looks through his device. So, while the lack of control certainly threatens privacy it does not necessarily involve its loss. I will henceforth refer to this as the threatened loss counterexample” [emphasis added].

Finally, the operators of those social-media websites cannot access or misappropriate one’s personal information, as that would be a major violation of various existing data privacy laws, such as EU GDPR, Telecom Regulatory Authority of India (TRAI) guidelines and might also constitute a breach of contract. Therefore, “loss of control” over personal information cannot be equated to “loss of privacy”, unless there is proof that they accessed our personal information from their database, without our consent.

**Part IV. DOES RIGHT TO PRIVACY EXIST OVER “DOCUMENTED PERSONAL INFORMATION”**?

We shall answer the aforementioned question in the affirmative and therefore, explicitly depart from Parent’s “new definition” of Privacy. There does exist a similar right to privacy over “documented personal information” or in other words, information stored in public records or government archives. This right imposes a duty on the State to use all personal information/data collected under a law for legitimate purposes, and not “wrongfully” misappropriate or disseminate them to third-parties without our prior consent.

There is no difference in the duties imposed by the Right to Privacy on a private entity and the Government, with regard to unauthorized use of collected information for extraneous purposes. However, the right to privacy is not absolute in its operation against the State. In the Sections below (infra), we shall be discussing the scope of limitations that can be imposed on the right to privacy by the State.

---

272 Asuncion Esteve, The business of personal data: Google, Facebook, and privacy issues in the EU and the USA, 7 International Data Privacy Law (2017).
Part V. SCOPE OF LIMITATIONS ON PRIVACY IN INDIA

The 9-judge bench of the Indian Supreme Court in Puttaswamy (2017) unanimously held that right to privacy is a fundamental right, by virtue of being an “intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution”.276

There were varying opinions regarding what would be the most befitting test to examine the legality of State intrusions into Privacy. However, the test laid down by Justice Chandrachud277 at page 264, also supported by Justice Kaul278 at para 71 of his judgement, should be considered as the majority opinion. In the subsequent Aadhaar judgement, the majority opinion affirmed the above conclusion at para 89.279 Therefore, the test is as follows:280

i. The action of the State must be empowered by a Law
ii. The proposed action must be necessary and also pass the test of legitimate aim
iii. The extent of interference with individual’s privacy must be proportionate to the need for such interference
iv. The law in question must also provide procedural guarantees against abuse of such interference.

Kaul J. had suggested that Indian Government could consider data privacy laws of the European Union,281 in order to facilitate safeguards against data infringement. The judges have also recognized “legitimate aims” of the State to include- National Security, identifying and prosecuting criminal activities, situations that require Privacy to be balanced with other fundamental rights.282 Moreover, the above exposition had a significant impact on two aspects- first, the idea of “coerced consent” covered under the pretence of providing social and monetary benefits and second, State Surveillance.

---

276 Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017 (10) SCALE 1, at Pg. 546 [Operative Order].
277 Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017 (10) SCALE 1, Conclusion 3(H) of Chandrachud J.
278 Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017 (10) SCALE 1, ¶ 71 of S.K. Kaul J.
279 K.S. Puttaswamy v. Union of India, 2018 (12) SCALE 1, ¶ 89 of Sikri J.
280 K.S. Puttaswamy v. Union of India, 2018 (12) SCALE 1, ¶ 89 of Sikri J.
282 Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017 (10) SCALE 1, ¶¶ 13, 14, 72, 73 of S.K. Kaul J.; ¶¶ 180, 181 and Conclusion (5) of Chandrachud J.
A. **COERCED CONSENT**

The right to informational privacy has been explicitly recognized by Puttaswamy. This right inheres the liberty of individuals to *not be coerced* into giving consent for a State welfare program. In other words, individuals possess the right of “informed consent” and can willingly give up their personal data, if they want to avail the benefits under a social welfare scheme.

This point has been immaculately articulated by **Justice Kaul** at para 70, wherein he held that the “*State must ensure that information is not used without the consent of users and that it is used for the purpose and to the extent it was disclosed.*”\(^{283}\) In order to provide an illustration, he gave an example of posts on social media and observed that personal data revealed via such posts “*is meant only for a certain audience, which is possible as per tools available, then it cannot be said that all and sundry in public have a right to somehow access that information and make use of it.*”\(^{284}\)

Finally, if an individual has willingly parted with his/her personal data in exchange of social and monetary benefits, then according to **Chandrachud J.**, the State must utilise the collected data solely for “*legitimate purposes of the state*” and refrain from any unauthorised use of such data for “*extraneous purposes*”.\(^{285}\)

B. **SURVEILLANCE**

A close reading of the Puttaswamy judgement shall reveal that the Indian Supreme Court has not brought down the curtain on State surveillance, but *only limited* the circumstances warranting collection and analysis of personal data.

The Supreme Court, via the above proportionality test, laid down a framework within which every State policy intruding into individual privacy must be “narrowly tailored”. The chances of mass surveillance policies passing constitutional muster have been significantly diminished, however, the possibility of State conducting targeted surveillance is still alive. In any event, the State is under an obligation to ensure that every such policy provides for sufficient safeguards and surveillance is used as a measure of last resort.

According to the judgement, Data collection, data analysis and data mining by the State *may* pass muster in the following instances:

\[^{283}\] Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017 (10) SCALE 1, ¶ 70 of S.K. Kaul J.

\[^{284}\] Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017 (10) SCALE 1, ¶ 70 of S.K. Kaul J.

\[^{285}\] Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017 (10) SCALE 1, ¶ 181 of Chandrachud J.
i. **National Security** [Justices Chandrachud and Kaul];

ii. **Legitimate State interest, such as preventing and investigating criminal activities** [Justices Chandrachud and Kaul];

iii. **Social welfare schemes, “with the object of ensuring that resources are properly deployed to legitimate beneficiaries”** [Justice Chandrachud].

Therefore, while the Indian Supreme Court has explicitly recognised Privacy as a fundamental guarantee under the Constitution, it has also recognized the legitimate interests of the State in infringing individual privacy in certain exceptional circumstances.

**Part VI. STATE SURVEILLANCE VS. INDIVIDUAL’S RIGHT TO PRIVACY: A TOUR D’HORIZON**

(a) **American Jurisprudence**

The US Supreme Court in *Whalen v. Roe* adjudicated on whether a State information collection and data bank storage scheme violated individual privacy interests. Furthermore, the Court considered a hypothetical right to informational privacy, but did not declare informational privacy as a right.

The standard used by the US Supreme Court in *Whalen* for testing the constitutionality of the legislative action is similar to the three-fold proportionality test laid down by the Indian Supreme Court in *Puttaswamy*. The Court in *Whalen* observed that due to statutory limitations, sufficient safeguards were present against the abuse of this data. However, to differentiate *Whalen* from the *Aadhaar* in India, it has been observed that there is a lack of criminal procedural safeguards to protect infringement of the information collected under *Aadhaar*.

Many decades after the *Whalen v. Roe* decision, the court in *NASA v. Nelson* got an opportunity to adjudicate on questions of law concerning right to informational privacy. The Court was adjudicating on whether a governmental background check violated a right to informational privacy by compelling employees to disclose past use of illegal drugs.

---

286 Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017 (10) SCALE 1, ¶¶ 13, 14, 72-3 of S.K. Kaul J.; ¶ 180-1 and Conclusion (5) of Chandrachud J.

287 Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017 (10) SCALE 1, ¶¶ 13, 14, 72-3 of S.K. Kaul J.; ¶ 180-1 and Conclusion (5) of Chandrachud J.

288 Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017 (10) SCALE 1, ¶¶ 180-1 and Conclusion (5) of Chandrachud J.


However, the Court in the case answered the question in negative, holding that no such right was violated.

In United States v. Jones, Sotomayor J. in her separate opinion had observed that right to privacy can be violated via the use of GPS system, without even causing trespass. However, the majority went on the lines of trespass as the justification for finding an unconstitutional encroachment of private information rather than on the lines of informational privacy. Therefore, with regard to the US Jurisprudence, it appears that right to informational privacy is yet to be recognized expressly as being protected under the US Constitution. Although, the parameters on which it could be tested is well grounded in the Whalen decision.

(b) UK Jurisprudence

The famous Calcutt Committee Report had defined “privacy” as “The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication.” United Kingdom being a signatory to the European Convention on Human Rights had ratified and incorporated the Convention in its domestic legislation i.e. Human Rights Act 1998. Schedule I of the Act contains the Convention which is to be interpreted with other provisions of the Act. Article 8 of the Convention provides that “Everyone has the right to respect for his private and family life, his home and his correspondence”. While this recognizes the existence of privacy, a direct claim for violation of privacy under Article 8 of the Convention cannot be raised in UK. However, various judicial decisions such as the House of Lords in Campbell decision and the England and Wales Court of Appeal in Vidal-Hall v. Google decision, have held that a tortious claim for misuse of private information can still be brought to the courts.

The UK Supreme Court in PJS v. News Group Newspapers had held that there are two primary components which are covered by misuse of private information. The two components are (i) The confidentiality component (protecting the secrecy of private information); and (ii) The intrusion component (preventing intrusion into an individual's

---

293 The Human Rights Act 1998, Schedule I (United Kingdom).
privacy). The Court further held that an interim injunction can be used to prevent further disclosure of private information\textsuperscript{297}.

The Data Protection Act, 1998, serves as another legislation which can be used for protection of private information in the UK. The England and Wales Court of Appeal in PJS v. News Group Newspapers\textsuperscript{298} held that an individual could claim compensation if use of their private or personal information contravenes the Data Protection Act provisions and this is not merely limited to financial claims; it can cover compensation for distress.

While the UK did not utilize the proportionality test in reference to informational privacy or any constitutional claims of violation of right to privacy, we can rely on the Privy Council decision in Elloy de Freitas\textsuperscript{299} which laid down a three-step proportionality test for legislative encroachments upon fundamental rights. The Privy Council held that the following parameters must be considered while deciding the legality of a legislative action: (i) whether the legislative objective is sufficiently important to justify limiting a fundamental right; (ii) whether the measures designed to meet the legislative objective are rationally connected to it; and (iii) whether the means used to impair the right or freedom are no more than is necessary to accomplish the objective\textsuperscript{300}. Furthermore, the House of Lords in Huang\textsuperscript{301} had added a fourth requirement to those laid down in Elloy de Freitas, which stated that “the need to balance the interests of society with those of individuals and groups” must be considered.

The third parameter of the test laid down by UK courts is similar to the one accepted by the Indian Supreme Court in Puttaswamy, which states that the means used by the State must be proportional to the object and purpose sought to be achieved by the law under consideration. However, if we were to attempt a comparative evaluation of the type of proportionality test accepted by the Supreme Court of India as compared to the House of Lords in UK, it would be much easier for UK Parliament to create surveillance programmes. This is due to the fourth parameter stated in Huang\textsuperscript{302}, which allows the interests of individuals and groups to be balanced and potentially be superseded by the interests of the society.

\textsuperscript{298} Google Inc. v. Judith Vidal-Hall and Others, [2015] EWCA Civ 311 (England and Wales Court of Appeal).
\textsuperscript{299} Elloy de Freitas v. Permanent Secretary of Ministry of Agriculture, Fisheries, Lands and Housing, [1999] 1 AC 69.
\textsuperscript{300} Elloy de Freitas v. Permanent Secretary of Ministry of Agriculture, Fisheries, Lands and Housing, [1999] 1 AC 69.
\textsuperscript{301} The House of Lords in Huang v. Secretary of State for the Home Department, [2007] UKHL 11 (2007).
\textsuperscript{302} The House of Lords in Huang v. Secretary of State for the Home Department, [2007] UKHL 11 (2007).
(c) Canadian Jurisprudence

The Supreme Court of Canada in *R. v. Edwards Books* 303 had laid down three-fold standard while evaluating legislations encroaching upon fundamental rights - (i) the limiting measures must be carefully designed, or rationally connected, to the objective; (ii) the limiting measures must impair the right as little as possible; and (iii) their effects must not so severely trench on individual or group rights that the legislative objective, albeit important, is nevertheless outweighed by the abridgment of rights.

The Canadian Supreme Court in *Andrews* 304 relied on the *R. v. Edwards Books* decision to espouse a proportionality test while analysing the rights and freedoms guaranteed by The Constitution Act, 1982, of Canada. The Court held that it must consider (i) the nature of the right, (ii) the extent of its infringement, and (iii) the degree to which the limitation furthers the attainment of the legitimate goal reflected in the legislation. This is also famously known as the Andrews standard.

In Canada, the Privacy Act provides the confines within which the State can encroach upon the privacy of individuals via legislative action. The Privacy Act has been subjected to several judicial interpretations, such as the interpretation of the term “personal information”, as provided under Section 3 of the Privacy Act 305, by the Supreme Court of Canada in *Canada (Information Commissioner)* 306. Therefore, in Canadian jurisprudence any encroachment on the privacy of an individual will have to be understood in light of the Andrews standard and the Canadian Privacy Act 1985, as privacy has not been guaranteed as a fundamental right under the Canadian Constitution 307.

(d) South African Jurisprudence

South Africa is one of the few countries which explicitly recognizes the right to privacy of individuals in its Constitution. Section 14 of the South African Constitution 308 protects the right to privacy of individuals. It states that:

“Everyone has the right to privacy, which includes the right not to have:

(a) Their person or home searched;”

---

305 Privacy Act §. 3, RSC 1985, c P-21 (Canada).
306 *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, 2003 SCC 8 (Supreme Court of Canada).
307 The Constitution Act, 1982 (Canada).
(b) Their property searched;
(c) Their possessions seized; or
(d) The privacy of their communications infringed.”

Therefore, the South African Constitution has explicitly set out the confines of a constitutional right to privacy. The right to privacy in South Africa, much like other countries is not absolute. Justice Ackermann in Bernstein decision of the Constitutional Court of South Africa held that “the scope of a person's privacy extends ‘a fortiori’ only to these aspects in regard to which a legitimate expectation of privacy can be harboured.”

The South African Supreme Court of Appeal in the S. v. Nkabinde decision held that the monitoring of conversations between the accused and his legal representatives by the police violated the right to privacy protected under the South African Constitution. This can be justified under Section 14(d) of the South African Constitution. However, other private acts which must be protected under informational privacy, could potentially be protected by adopting an expansive reading of Clauses (a), (b) and (d) of Section 14.

CONCLUSION

In light of the aforesaid discussion, the following points can be agreed upon – (1) The current discourse on Privacy lacks the necessary clarity; (2) There is a need to redefine the contours of Privacy or a ‘right to privacy’ in order to avoid confusion with other constitutional values such as, liberty, autonomy, dignity etc.; (3) Whenever there is a question of State Surveillance, there are multiple competing interests at play – State (Government) interest, Public interest, Individual interest, and the Courts must adopt a fine adjudication strategy to be able to balance all three in a manner that the equilibrium remains undisturbed; (4) The boundaries of right to privacy must be made amply clear to the Public, so that they can accordingly tweak their conduct.

For point (2), we have proposed a fresh definition of Privacy [Refer Part II], which we believe might be able to plug the existing gaps in the existing framework. In conclusion, let

310 Bernstein and others v. Bester and Others, NNO 1996 (2) SA 751 (CC) (Constitutional Court of South Africa), ¶75.
us end with the words of Justice Sanjay Kishan Kaul\textsuperscript{312} - “Let the right of privacy, an inherent right, be unequivocally a fundamental right embedded in part-III of the Constitution of India, but subject to the restrictions specified, relatable to that part. This is the call of today. The old order changeth yielding place to new”

\textsuperscript{312} Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017 (10) SCALE 1, ¶83 of S.K. Kaul J.